Security zSecure Admin and Audit for RACF
Version 1.13

Getting Started

GI11-9162-00

Security zSecure Admin and Audit for RACF
Version 1.13

Getting Started

GI11-9162-00

Note
Before using this information and the product it supports, read the information in Appendix B, "Notices," on page 107.

November 2011

This edition applies to version 1, release 13, modification 0 of IBM Security zSecure Admin for RACF (product number 5655-T01) and IBM Security zSecure Audit for RACF (product number 5655-T02) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

IBM Security zSecure Admin and Audit for RACF® (Resource Access Control Facility) automates many of the recurring administrative tasks and audit reporting for RACF systems. These products rely on the zSecure Collect program to collect and analyze data from RACF and z/OS® systems, enabling you to easily monitor user access privileges, implement scoping to limit administrator privileges, and to audit user behavior. These products also enhance the administrative and reporting functions of RACF systems, facilitating security monitoring and decentralizing system administration.

This document is intended to help you learn the basics of using IBM Security zSecure Admin and Audit for RACF. After working through this document, you should have a working understanding of these products and the ability to explore other product features.

Intended audience

The target audience for this book includes security administrators and mainframe system programmers. Readers of this book should have working knowledge of RACF systems administration and be comfortable using Interactive System Productivity Facility (ISPF).

What this publication contains

The purpose of this document is to help you quickly become familiar with IBM Security zSecure Admin and Audit for RACF. This document is not a full reference manual and does not cover all features. The material focuses on the interactive features (using ISPF panels) and highlights the major functions of IBM Security zSecure Admin and Audit for RACF.

Except for a few introductory pages, this document is intended as a hands-on guide while you work with IBM Security zSecure Admin and Audit for RACF. The publication explains how to use IBM Security zSecure Admin and Audit for RACF to perform common administration tasks and how to audit and run reports on RACF systems.

Related Documentation

For more detailed information about the IBM Security zSecure Admin and Audit for RACF components, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* (document number LC14-7663-00).

This publication is provided on the *IBM Security zSecure: Documentation CD* (LCD7-1387-09). You can download the documentation CD when you order and download IBM Security zSecure Admin and Audit for RACF from the ShopzSeries website or from the ESW download site. To obtain electronic or printed copies of these manuals, see the instructions in “Ordering publications” on page vi.

Release information

The zSecure Release Information topics include details on new features and enhancements, incompatibility warnings, and documentation update information

for your zSecure product. You can review the most current version of the release information in the zSecure Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

Accessing terminology online

The IBM® Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessing publications online

The *IBM Security zSecure: Documentation CD* contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli® products, as they become available and whenever they are updated, to the Tivoli Documentation Central website at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Select http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Licensed publications

Licensed publications are indicated by a publication number that starts with *L* (LC14-7663-00, for example). To obtain PDF or printed copies of licensed publications, send an email requesting the publication to:

tivzos@us.ibm.com

Include the following information:

- IBM customer number
- List of publication numbers that you want to order
- Preferred contact information

You will be contacted for further instructions for fulfilling your order.

For details, see "Support for problem solving."

Accessibility

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use software products successfully. For keyboard access in the Tivoli zSecure z/OS products, standard shortcut and accelerator keys are used by the product, where applicable, and are documented by the operating system. See the documentation provided by your operating system for more information.

Visit the IBM Accessibility Center at http://www.ibm.com/alphaworks/topics/accessibility/ for more information about IBM's commitment to accessibility.

Tivoli technical training

For Tivoli technical training information, see the IBM Tivoli Education website at:

http://www-01.ibm.com/software/tivoli/education/.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the link for the Tivoli Users Group at http://www.tivoli-ug.org.

Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Navigate to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Support Assistant
The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the Support Assistant software, navigate to http://www.ibm.com/software/support/isa.

Conventions used in this publication

This publication uses several conventions for special terms and actions and operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multi-column lists, containers, choices, names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, directory names, and path names
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Chapter 1. Overview

IBM Security zSecure Admin for RACF and IBM Security zSecure Audit for RACF are two distinct but complementary products that you can use to administer and audit RACF systems.

zSecure Admin provides RACF management and administration at the system, group, and individual levels along with RACF command generation. zSecure Audit provides RACF and z/OS monitoring, Systems Management Facility (SMF) reporting, z/OS integrity checking, change tracking, and library change detection. Both products provide displaying, reporting and verifying functionality for RACF profiles and show the z/OS tables that describe the Trusted Computing Base (TCB). Figure 1 shows the functionality available in each product and shows the complementary functionality provided in both products.

zSecure Admin and zSecure Audit for RACF are licensed individually, but can be used together.

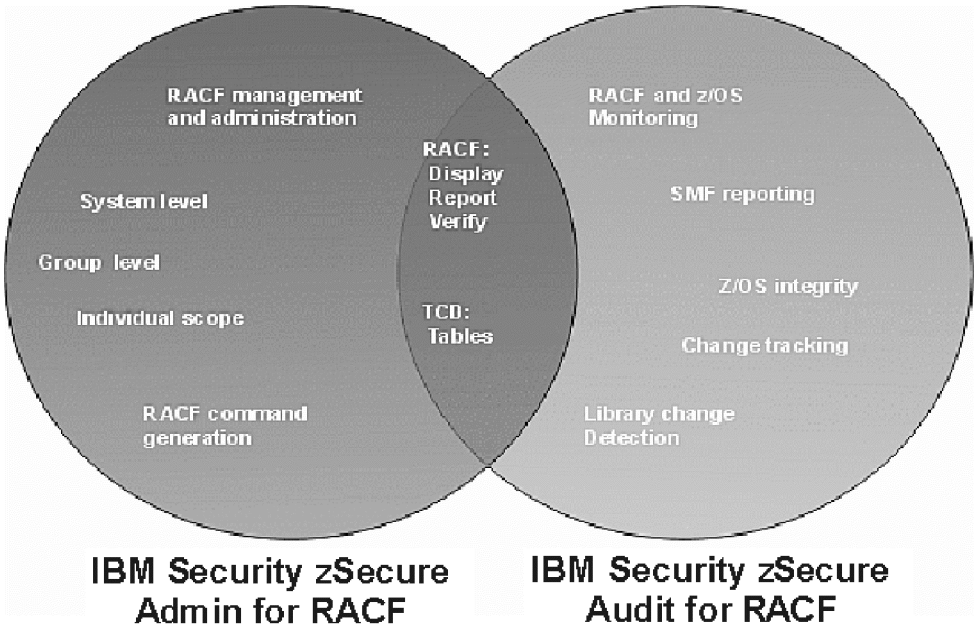

Figure 1. zSecure Admin and zSecure Audit product functions

The primary processing programs are large modules that can be used in batch or interactive mode. Interactive mode is most common, although batch mode can be useful for automated, periodic checks and for producing daily reports.

zSecure Admin and zSecure Audit provide an interactive user interface implemented in ISPF using the *panel, skeleton* and *message* libraries supplied with zSecure. ISPF is the main program running during an interactive session, calling the zSecure application program as needed. The interactive panels call the `CKRCARLA` load module as needed.

Figure 2 on page 2 illustrates the general data flow for zSecure Admin and zSecure Audit. The user works through ISPF panels, which generate commands that are

sent to the CKRCARLA program. The program returns results that are displayed through ISPF panels.

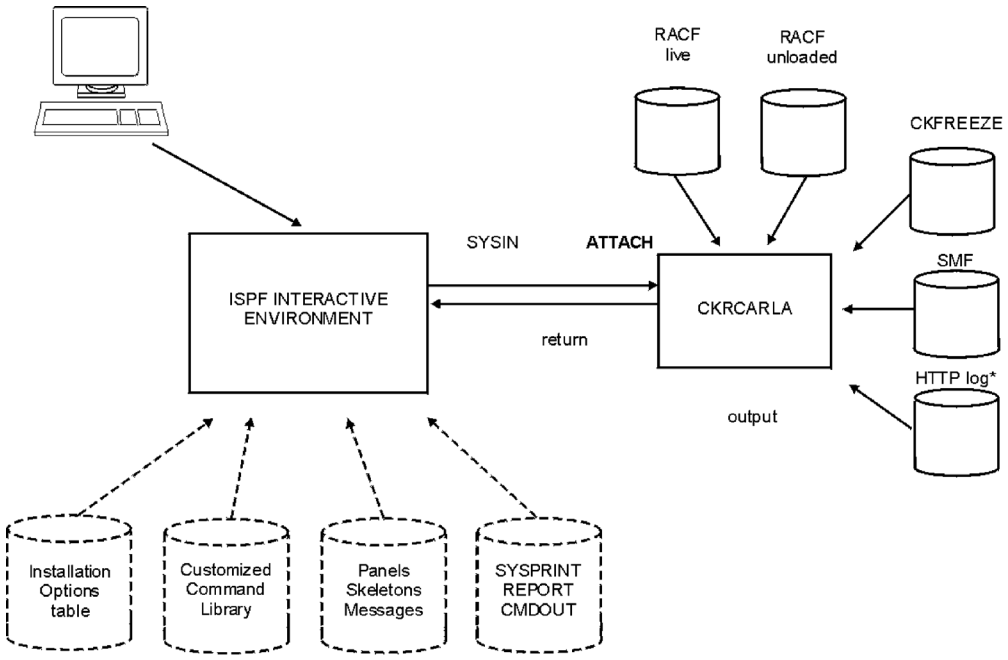

Figure 2. Conceptual data flow

This general design, with separate interactive and noninteractive components, has several practical advantages:

- It separates interactive interfaces from the application program. This separation gives you more flexibility in designing and using the interfaces and programs, especially when customizing the ISPF interface.
- Any functions that can be run interactively can also be run in batch mode.
- zSecure Admin and zSecure Audit for RACF can create customized reports using the CARLa Auditing and Reporting Language (CARLa) and run these reports from the ISPF panels.
- The products can be used remotely, in cases where a TSO connection is not possible or practical, in NJE networks, for example.

CARLa auditing and reporting language

zSecure Audit for RACF is command-driven using the CARLa Auditing and Reporting Language (CARLa). The commands are explained in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* (LC14-7663-00).

A typical user, using ISPF, does not need to be concerned with CARLa. The commands are generated automatically and sent to the application program. Except for the few comments in this section, this guide does not discuss the CARLa command language and concentrates on the use of zSecure Admin and Audit through ISPF.

The command language is generally used for the following reasons:

- To generate customized reports
- To use the product in batch mode

Because the standard reports are comprehensive, you might not ever need customized reports. Nevertheless, you can create customized reports. Batch use is attractive as part of a security monitoring function. For example, you can use a scheduled batch job to run monitoring checks and reports automatically.

A comprehensive set of sample reports is available in a data set referred to as the CARLa library (low-level qualifier of SCKRCARL and often referred to with the default ddname CKRCARLA).

Data sources

zSecure Admin and zSecure Audit for RACF use several different types of data. Figure 3 provides an overview of the data sources and processing performed by the products.

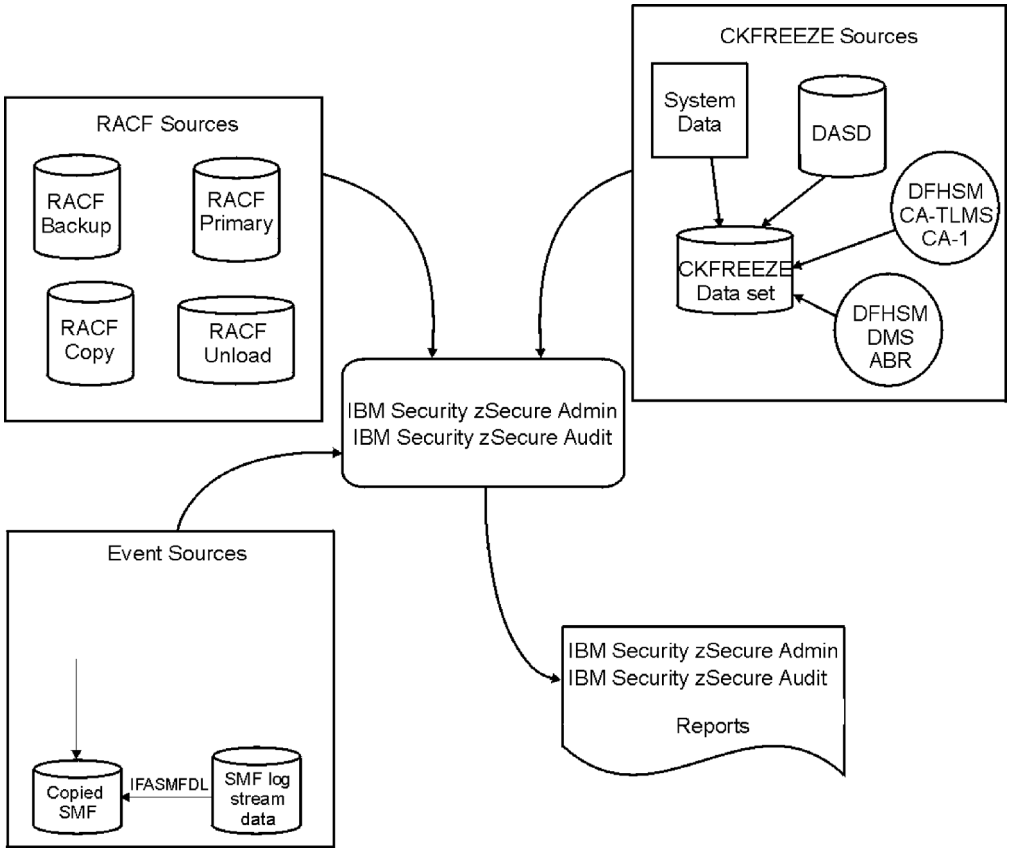

Figure 3. Data input sources

zSecure Admin and zSecure Audit for RACF usually require RACF data. This data can come from the following sources:

- The primary live RACF database
- The backup live RACF database
- Unloaded RACF data
- A copy of a RACF database, or an active RACF database from another system

zSecure produces unloaded RACF data by reading the live RACF database and creating a copy in a proprietary format suitable for high-speed searches.

If you are using zSecure Audit for RACF functions, the program might require SMF data. The SMF data can come from the live SMF data sets, SMF log streams, or from sequential SMF data sets produced with the IFASMFDP or IFASMFDL programs. These IBM programs unload SMF records from the live SMF data sets and SMF log streams respectively. Sequential SMF data sets can be on disk or tape, although many installations might not permit TSO users to mount tapes for interactive use. zSecure Audit cannot process pseudo-SMF files created by the RACF REPORT WRITER or the IRRADU00 SMF unload program.

CKFREEZE data sets

zSecure Audit for RACF uses DASD data provided by zSecure Collect. This program runs as a batch job and reads all online Volume Table Of Contents (VTOCs), VSAM Volume Data Set (VVDSs), catalogs, selected Partitioned Data Set (PDS) directories, and calculates digital signatures at the member and data set level when requested. It writes all this to a data set referred to as a CKFREEZE data set.

zSecure Admin and zSecure Audit for RACF also use z/OS control block data. zSecure Collect gathers this data at the same time that it gathers DASD data. It uses APF-authorized functions to retrieve data from other address spaces and from read-protected common storage. Additionally, batch collection permits analysis of a remote system where the data was collected.

You define input sets for zSecure Admin and zSecure Audit for RACF. For example, one set might consist only of the live RACF data. Another set might use live RACF data plus a CKFREEZE file. Another set might use unloaded RACF data, a CKFREEZE data set, and several SMF data sets. You can switch between input sets while in the ISPF environment.

Using remote data and command routing

Beginning with version 1.12, zSecure Admin and zSecure Audit support the use of remote data sets as input for creating reports and displays. Using this functionality, known as multi-system support, you can report on and manage multiple systems from a single session. This function is also integrated with zSecure Admin support for routing RACF commands using zSecure services or RACF Remote Sharing Facility (RRSF) services.

Using remote data for creating reports is useful for ad hoc reporting about profiles or settings. However, this access method is less suited for queries that require processing of the entire security database or the entire CKFREEZE data set because it takes longer to access large amounts of remote data than to access the same data locally.

To use the multi-system support functionality, your environment must have an active zSecure Server, which runs in a separate server address space. This server performs the necessary functions for communicating with remote systems to route commands and access RACF databases, SMF input files, CKFREEZE data sets, and other defined data sets. For more detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

Chapter 2. Learning basic operations

Review the following procedures to learn how to start the zSecure Admin and Audit applications and to navigate, select, input, and manage RACF data. You can read about the following tasks:

- Viewing, managing, and maintaining RACF profiles for user, groups, and data sets
- Managing access rights
- Reporting on digital certificates
- Comparing users

Before you begin

Follow the procedures outlined in this section before you start using zSecure Admin and zSecure Audit for RACF.

Checking TSO logon parameters

Make sure that you are logged on to TSO with a large enough region size. zSecure Admin and zSecure Audit for RACF use virtual storage to reduce I/O and to improve the response time. The amount of virtual storage depends on the size of your installation and on the information you requested. A good region size value to start with is 32 MB.

Setting ISPF & 3270 format

zSecure Admin and zSecure Audit for RACF panels are designed to be used with 24-line and larger screens. To be most effective with 24-line screens, type **PFSHOW OFF** on the command line in any ISPF panel and press Enter to remove the program function key definition information that ISPF automatically places in the last one or two lines of the screen. Use the **PFSHOW ON** command to restore the PF key definitions.

Starting the products

After installing the products, you can start the zSecure Admin and Audit applications and perform typical tasks.

To get started, perform the following steps:

1. Type **6** on the **Option** line, and then press Enter to open ISPF Command Shell.
2. Enter the command **CKR** and press Enter.

   This command starts the combined zSecure Admin and zSecure Audit for RACF products. After you enter the command, the Main menu opens as shown in Figure 4 on page 6.

```
 Menu         Options       Info    Commands     Setup
_____________________________________________________________________________

                        zSecure Admin+Audit for RACF - Main menu
Option ===> ____________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex:   ACTIVE BKUP DB AND SMF

Product/Release
5655-T01 IBM Security zSecure Admin 1.13.0
5655-T02 IBM Security zSecure Audit for RACF 1.13.0
```

Figure 4. zSecure Suite - Main menu

The first time you enter this panel, only the major selection options are shown. (If necessary, use option **SE.R** to reset the Start panel to the Main panel.) To select an option, type the two-character abbreviation on the command line. Then, press Enter. Depending on the option selected, the menu either expands to show more detailed options or presents the submenu for the next selection.

The following sections show you how to use some of the display functions to ensure that the product is working correctly. At this point, your live RACF database is being used for input. Normally, using zSecure with the live RACF database does not cause any noticeable effects on production operations.

Maintaining RACF profiles

You can maintain RACF profiles by displaying an overview of the profiles and then selecting one on which to perform an action. The profile selection panels have fields, also known as *filters*, to select or to exclude data. By default, everything is selected and nothing is excluded. To see an example, complete the following steps:

1. On the Main menu, type **RA** (RACF Administration) in the **Option** line, and press Enter to see the options for viewing and maintaining the RACF database.
2. Type **G** (Group) in the Option line, and press Enter without entering any parameters in the panel.
3. At the default prompt, press Enter again.

After completing this procedure, zSecure Admin and zSecure Audit for RACF shows everything in the RACF database relevant to the function of the panel; group profile information in this example. You can reduce the amount of data shown in the panel by specifying one or two selection or exclusion parameters.

Tip: You can use the FORALL primary command on a record-level display to specify a command to be applied to all profiles on the current display. Without a parameter, primary command FORALL displays a panel where a command can be entered. You can also enter the command directly on the FORALL command.

This example uses the live RACF database to demonstrate the speed and non-interference of zSecure Admin and Audit when using the live RACF database.

"Adding data" on page 47 guides you through the creation of an unloaded RACF database. The unloaded database is used for the text and examples in the remainder of this guide.

This section introduces the facilities offered by zSecure Admin to maintain the RACF database. The examples show how easy it is to use the zSecure ISPF interface and to control the RACF or CKGRACF commands that the product generates in response to the commands issued from the interface.

zSecure Admin helps you maintain profiles at the group and user level as well as at the single-entry level. You can quickly find out about the structure of groups and users, and modify structures based on your organizational structure.

After you learn how to use the interface and manage commands, you will learn about general maintenance functions, devolved maintenance and how the help desk can shift workload–by enabling password maintenance without having the special authority, for example.

Displaying user profiles

To open the User Selection panel to view and manage user profiles, complete the following steps:

1. If you are not in the Main menu, press PF3 to return to the Main menu.
2. Type **RA** (RACF Administration) in the Option line, and press Enter to see the options for viewing and maintaining the RACF database.
3. From the RA menu, select option **U** (User). Then press Enter to open the User Selection panel; see Figure 5 on page 8.

   This panel provides some of the most frequently used selections. It consists of the following parts:

   - Add new user or segment
   - Additional selection criteria
   - Output/run options

   Depending on the additional selection criteria or output/run options you choose (by placing a / in front of one of those options), you might be taken to another panel to specify additional selection criteria. After making your selection, press PF3 to return to the User Selection panel, or press Enter if you want to execute the query.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
       zSecure Admin+Audit for RACF - RACF - User Selection
Command ===> ____________________________________________________   _ start panel

_   Add new user or segment

Show userids that fit all of the following criteria
Userid  . . . . . . ________     (user profile key or filter)
Name  . . . . . . . ____________________________ (name/part of name, no filter)
Installation data . ____________________________ (data scan, no filter except *)
Owned by  . . . . . ________     (group or userid, or filter)
Default group . . . ________     (group or filter)
Connect group . . . ________     (group or filter)

Additional selection criteria
_  Other fields       _  Attributes       _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Specify scope
_  Print format          Customize title     Send as e-mail
      Background run     Full page form      Sort differently     Narrow print
```

Figure 5. User Selection panel

4. In the **Userid** field, type your userid.

   Tip: The additional print options are available only if the **Print format** field is activated. To activate this field, type **/** in the **Print format** selection field.

5. Press Enter.

   zSecure Admin and Audit for RACF searches the RACF database and opens the user profile overview panel as shown in Figure 6.

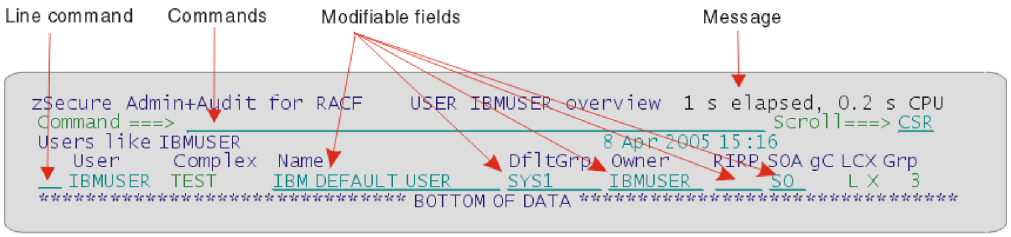

Figure 6. Overview display for selected user

The message in the upper right line of the panel provides performance information indicating the elapsed and CPU time used to execute the query.

This overview display shows each selected user profile on a single line. If applicable you can scroll up and down, left and right, to view additional information.

Some of the field values can be edited: entries in the **Name** column, for example. Depending on your ISPF option settings and terminal type, fields that can be edited (modified) are indicated by underscores or might be shown in a color that is different from the color for fields that cannot be edited (the **User** field, for example). If you type a new value over a modifiable field, zSecure Admin generates the appropriate native RACF command to change the profile to the new value.

Note: If desired, you can change the ISPF display colors in most panels using the following procedure:

a. Select **Options** from the menu bar.

b. From the Options menu, select **1. Settings**.
c. Select the **Colors** from the bar. Then select **2. CUA attributes**.

After specifying the changes, press Enter to apply them. The changes become effective the next time you run a query.

Due to limited space, the labels in the profile display are abbreviated as shown in Table 1.

Table 1. Profile display label descriptions

Label	Description
RIRP	Flag fields that indicate if the profile is **R** Revoked, **I** Inactive, **R** Restricted, or **P** Protected
SOA	Shows the settings for the following attributes: **S** Special, **O** Operations, and **Au** Auditor
gC	Show **g** group Authorities Present and **C**lass Authority Present
LCX	Indicates if the following conditions are true: `RACLINK` Present (**L**). User has a certificate (**C**). Password is expired (**X**).

These field descriptions are also available on the integrated help panels available in the ISPF interface. You can access panel-level help and field-level help on most panels. Panel help and field-sensitive help are available on all security database displays, at both the record level and detail level.

- For field help, position the cursor in the field of interest and press PF1.
- For panel help, position your cursor on the command line. Then press PF1.

Tip: Many of the zSecure data displays are wider than 80 characters. To scroll right or left, use the PF11 and PF10 keys.

To display more detailed information about a profile, complete the following steps:

1. Move the cursor to the beginning of the displayed profile line (in the line command field). Then, press Enter.

   To select an entry in the panel, you can use either of the following methods:

   - Position the cursor on the line command field, and then press Enter.
   - Enter the **S** command and then press Enter.

   Additional line commands such as **C** (copy) and **D** (delete) are also available. These commands are covered later in this guide.

   Tip: If you are unsure about the available line commands on a certain profile, type a **/** and press Enter; this action opens a panel showing all applicable line commands.

   Tips:

   a. If you are unsure about the available line commands on a certain profile, type a **/** and press Enter; this action opens a panel showing all applicable line commands.
   b. You can use the FORALL primary command on a record-level display to specify a command to be applied to all profiles on the current display. Without a parameter, primary command FORALL displays a panel where a command can be entered. You can also enter the command directly on the FORALL command.

2. To return to the User Selection panel, press PF3. (Press it twice if you are in the detail overview.)

Now try something a little more interesting, such as entering `SYS*` in the **Userid** field to display all user profiles that start with `SYS*`. You can inspect the details for these users by selecting any displayed user profile line. If you have appropriate authority for the RACF database, you can change many of these fields by editing the field value in the panel. When you specify a new value, zSecure performs checks to prevent accidental changes. For the purpose of the example, do not attempt to make any changes now.

Note: When specifying selection criteria in a field, you can use the generic characters asterisk (*) and percent sign (%).

User selection panel details

The User Selection panel is split into the following sections:

- Use the first section to add a new user or segment.
- Use the second section to specify the most commonly used RACF management selection criteria.
- Use the third section mostly to report on the RACF database using more advanced selection criteria. For example, you can report on all user profiles that have the SPECIAL and OPERATIONS attributes.
- Use the fourth section to can customize the resulting output from your query.

To select fields for the advanced selection criteria (third section) and output customization (fourth section), place a **/** next to the field desired. Then, press Enter.

Note: Most of the fourth section of the panel can be modified only if the **Print format** field has been selected by placing a **/** in front of it and pressing Enter. Before you can use the **Send as e-mail** option in this section, you must specify SMTP configuration parameters in the Setup output definition panel, as described in “Setting up Output” on page 52. For now, continue without selecting the **Print format** option.

zSecure displays any user profile that matches the criteria you enter in the User Selection panels. If nothing is specified for a particular field, that field is ignored during the search. Several fields accept **/**. The **/** means that the option is selected, and profiles matching the specified parameter or parameters are displayed (or an additional selection panel is displayed). Most fields also accept the **S** command to activate the selection option. Blank means that the option is ignored for selecting profiles.

For example, typing **/** in the **Attributes** field opens the User Attributes panel illustrated in Figure 7 on page 11.

```
  Menu         Options       Info    Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - RACF - User Attributes
Command ===> ____________________________________________________________
All users
Specify groups of criteria that the userids must meet:
Systemwide and group authorizations
OR      _   Special        _   Operations     _   Auditor      _   Class auth
        _   Group-special _   Group-oper     _   Group-audit

Logon status
OR      _   Revoked        _   Inactive       _   Protected    _   Passw expired
        _   Revoked group _   Certificate    _   Pass phrase  _   Phrase expired
        _   When day/time _   ID mapping

User properties
OR      _   Has RACLINK    _   Restricted     _   User audited _   Mixed case pwd

CKGRACF features
OR      _   Queued cmds    _   Schedules      _   Userdata     _   MultiAuthority

Connect authority . __     _  1. Use   2. Create   3. Connect  4. Join
```

Figure 7. User Attributes panel

To display all user profiles having system-wide authority, type **/** in the **Operations** field of the **Systemwide and group authorizations** section. Then, press Enter. This operation shows all user profiles that have system-wide `Operations` authority.

In the **Connect authority** field, you can select a user based on the specified connect authority. Only users that have at least one group connection that satisfies the comparison operator applied to the connect authority will be shown. You can use the comparison operators shown in Table 2.

Table 2. Comparison operators for **Connect authority** *field*

Operator	Description
<	Less than the access specified
<=	Less than or equal to (at most) the access specified
>	More than the access specified
>=	More than or equal to (at least) the access specified
=	Exact access
~= or <>	All but the specified access

Tips: zSecure Admin and zSecure Audit for RACF combine all the properties you specify with `AND` logic except when otherwise indicated.

Besides using **/**, you can also use **Y** and **N**. By specifying the `AND` operator and using `Y` and `N` values in the input fields within a group, you can find users that have the attributes selected with `Y` that have none of the attributes selected with `N`.

The **Revoked** option in the section **Logon status** checks for currently revoked users.

The **Password interval** field checks for users who are subject to password expiration. This field is available on the panel that displays when you specify / in the **Other fields** field on the RA.U panel. After selecting this field, press Enter to open the User Attributes panel to specify the attributes for selecting data. Try

searching for users with a non-expiring password and `SPECIAL` authority, or for users with non-expiring passwords and `Operations` authority. If you find any such users, other than possibly IBMUSER, you might investigate why they are defined this way.

As another example, you can type a **/** in the **Specify scope** field to examine the profiles within the scope of another userid or group. When you select this option, a panel opens for specifying the userid or group ID.

Using filters

In many panels, the input fields accept filters for selecting or excluding data. These are strings that can contain any of the following wildcard characters:

% Match one nonblank character.

***** Match any number of characters within a single string but not a dot, such as a single data set name qualifier or a user name.

****** Match any number of qualifiers at the end of a profile name.

: Search for specified characters within a name, but not used for class names or data set qualifiers.

zSecure Admin and zSecure Audit for RACF use Enhanced Generic Naming (EGN) notation, whether your RACF is in EGN mode or not.

Selecting dates

Several selection fields are meant for dates. You can use a variety of values and operators. However, all year values must be specified in four digits. Table 3 shows examples of date selection values and operators.

Table 3. Date selection values and operator examples

Operation	Meaning
= 04jul2004	July 4, 2004
< 04jul2004	Any day before July 4, 2004
= never	A date was never set
= today	Activity happened today
= today-3	Three days before today
< today-30	More than thirty days ago
>01jan2005	Any day after January 1, 2005

A date with the value DUMPDATE is the date your RACF database was unloaded. If you are using the live RACF database, specifying the value DUMPDATE is the same as using the value TODAY.

Note: When entering dates in selection fields, you must specify an operator in the small, two-character input field and the date value in the larger field.

Showing application segments

To show application segments, enter the action command **SE** in front of a user profile.

A panel opens with a list of application segments defined for this user.

Tip: Instead of using the **SE** action command, you can type a **/** in front of **Show segments** in the **Output/run** options **Show segments** section of the selection panel. This action opens a User Segments panel so that you can specify which segments you want to see. If you select **Segment presence** together with the **Show segments** field in the **Additional selection criteria** section, a panel opens with a list of segments. You can select a segment and specify additional selection criteria based on segment information. For example, you can select users based on output settings in the TSO segment.

Displaying group profiles

This section describes the procedure to display group profiles and query group profiles.

To display group profiles, complete the following steps:

1. Return to the Main menu by pressing End or Return.
2. From the RA menu, select option **G** (Group). Then, press Enter to open the Group Selection panel.

   This panel, shown in Figure 8, provides some of the most frequently used selections applicable to group profiles. Like the User Selection panel, this panel has the following sections:

   - **Add New Group or Segment**,
   - The common selection criteria,
   - **Additional selection criteria**
   - **Output/run options**

   Depending on the additional selection criteria or output and run options you select with the **/** character, you might be taken to another panel to specify additional selection criteria. After making your selection, press PF3 to return to the Group Selection panel.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
          zSecure Admin+Audit for RACF - RACF - Group Selection
Command ===> ____________________________________________________   _ start panel

_   Add new group or segment

Show groups that fit all of the following criteria
Group id  . . . . . ________     (group profile key or filter)
Owner . . . . . . . ________     (group or userid, or filter)
Subgroup of . . . . ________     (group or filter)
With subgroup . . . ________     (group or filter)
Installation data . ______________________ (data scan, no filter except *)

Additional selection criteria
_  Profile fields     _  Connect fields   _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Expand universal  _  Specify scope
_  Print format          Customize title    Send as e-mail
      Background run     Full detail form   Sort differently     Narrow print
      Print connects     Print names        Print subgroups
```

Figure 8. Group Selection panel

3. In the **Group id** field, type your default group or a group name string; for example, type `ABC*` for all group profiles starting with the string `ABC` in the **Group id** field.

4. Press Enter to search the RACF database and display the group profile(s) information in the Group Overview panel.

   The display, shown in Figure 9, looks very similar to the User selection overview except that it now shows different columns and Group profiles instead of User profiles.

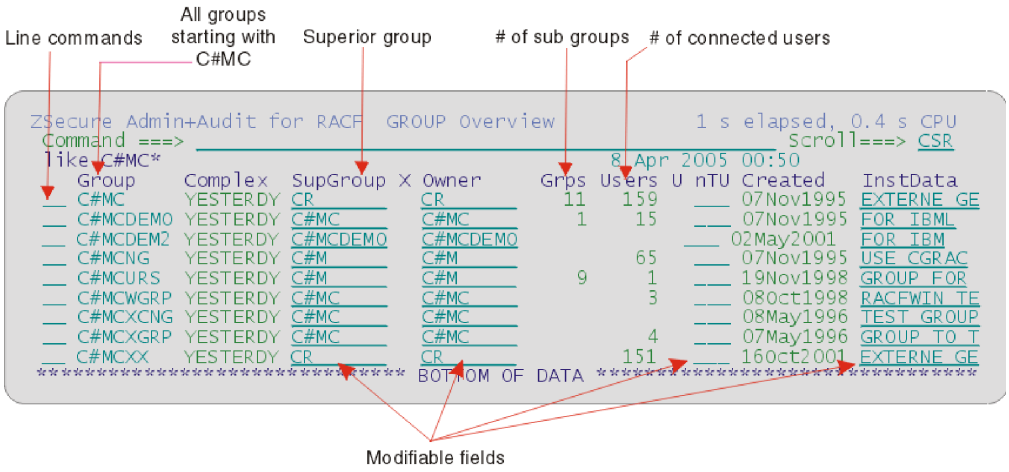

Figure 9. Group Overview panel

Using universal groups

All RACF profiles have a maximum size. The connect information for all connected users is stored in a normal Group profile. This implies that there is a maximum number of users that can be connected to a Group profile. The maximum number is approximately 6000 users. For very large RACF databases, this number might not be sufficient. This is the reason for the *universal* group. When the UNIVERSAL attribute is assigned to a Group profile, users with a *default connection* (connect to the group with USE authority and no connect attributes) are no longer stored in the Group profile. Only users that have a connect attribute like group-SPECIAL or group-OPERATIONS, or a connect authority exceeding USE, are stored in the Group profile.

The advantage of the universal group is that an unlimited number of users can be connected to this universal Group without its reaching the maximum size of a Group profile. So in large RACF databases, it is no longer required to split a very large Group by making a copy of the Group and connecting additional users to this new Group.

The disadvantage of the universal Group is that, when displaying the Group profile, you cannot determine which users are connected to the Group without searching all User profiles to find the users that are actually connected to this universal Group. In zSecure Admin and zSecure Audit you can automate this search using the *Expand universal* feature.

Note: Using this feature implies a full database read, and can cause the response time to be much longer.

There are two fields related to the UNIVERSAL attribute of Group profiles: **Universal Group** and **Expand universal**. If you enter a **/** before Profile fields, a panel similar to the one shown in Figure 10 on page 15 opens.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - RACF - Group Selection
Command ===>
All profiles
Show groups that also fit all of the following criteria:
Selection by date
Creation date . . . __   ___________           (date: yyyy-mm-dd/ddMMMyyyy/
                                                     DUMPDATE/DUMPDATE-nnn/
                                                     TODAY/TODAY-nn/NEVER)


Miscellaneous fields
Complex . . . . . ________     (complex name or filter)
# connected users . __   ____                 (operator: < <= > >= = <> = ¬=)
# subgroups . . . . __   ____

Enter "/" to specify selection criteria
_  Universal group
_  Queued commands
_  Userdata
```

Figure 10. Group profile field selection panel

To use the universal groups feature, perform one of the following actions:

- On the panel shown in Figure 10, type a **/** in the **Universal group** field.

  This selection searches the RACF database for universal groups only.
- Type a **/** in the **Expand universal** field in the Group Selection panel shown in Figure 8 on page 13.

  This selection causes all connected users, instead of just users with a non-default connect, to be displayed in the detail overview.

Tip: To see how the *Expand universal* option works, list a universal group twice: First list the group with the option enabled, and then list the group with the option disabled. Notice the differences in the lists of connected users.

Connecting and removing users

There are several ways to connect Users to a Group:

- Issue the **CO** line command (connect) in the Group or User profile overview panel.
- Use a **C** (copy) or **D** (delete) line command in the Group or User profile detail panel preceding a line containing connect details of a User or Group.
- Edit (overtype) the current values in the lines containing the connect information. This action generates a new connect command for the new value entered, and it generates a remove command for the overwritten value. If you do not want to execute the **Remove** command, delete it from the command confirmation panel before pressing Enter.

When the line command **CO** is used on a user or group profile, a Connect panel opens as illustrated in Figure 11 on page 16. (For Group profiles, you can add connections for up to 10 users in one operation.)

```
  Menu         Options       Info    Commands     Setup
_____________________________________________________________________________
                          zSecure Suite - RACF - Add connect
Command ===> ____________________________________________________________

Create new connect
Userid  . . . . . . . . CRMCKF1

Group . . . . . . . . . ________  (group or filter)

Optional connect attributes
Authority . . . . . . . ________  (USE ,CREATE ,JOIN or CONNECT)
Default UACC  . . . . . ________  (N/R/U/C/A)
Connect owner . . . . . ________
Future revoke date  . . ________  (MM/DD/YY)
Future resume date  . . ________  (MM/DD/YY)
_  Revoke
_  Special          _  Operations       _  Auditor

Enter a group for a single connect.
Leave the field blank or enter a filter (e.g. SYS*) to get a selection list.
```

Figure 11. Add / copy connect panel

Use the panel shown in Figure 11 to connect the User to another Group. In this panel, you cannot change the **Userid** field. When the **CO** command is issued for a Group profile, the **Group name** field cannot be modified instead.

Optionally, you can specify connect attributes in the lower half of the panel.

When using line command **C** instead of **CO** on a User or Group profile detail panel, you can connect the same User to another Group or connect another User to the same Group. It is even possible to modify both the **Userid** and the **Group** fields in the connect panel at the same time, connecting another User to another Group.

Reviewing dataset profiles

This section describes how to view dataset profiles, enable warning mode, and view and manage the access control list.

To display dataset profiles, complete the following steps:

1. To return to the Main menu, press Exit (PF3) in the Group Selection panel.
2. Select Option **D** to open the Data set Selection panel.

   You are still in the RACF subselection. This panel, shown in Figure 12 on page 17, is normally used to inquire about dataset profiles.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
       zSecure Admin+Audit for RACF - RACF - Data set Selection
Command ===> ____________________________________________________   _ start panel

_   Add new DATASET profile or segment

Show dataset profiles that fit all of the following criteria
Dataset profile . . ____________________________________________  1 1 EGN mask
Owned by  . . . . . ________     (group or userid, or filter)       2 Exact
High level qual . . ________     (qualifier or filter)              3 Match
Installation data . ________________________ (substring or *)     4 Any match

Additional selection criteria
_  Profile fields     _  Access list      _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Enable full ACL   _  Specify scope
_  Print format          Customize title     Send as e-mail
      Background run     Full detail form    Sort differently     Narrow print
      Print ACL          Resolve to users    Incl operations      Print names
```

Figure 12. Data set Selection panel

This panel is used in much the same way as the user profile panel. Specify criteria in as many or as few fields as you like. If nothing is entered in a field, then that field is not used as a selection or rejection criterion during the database search. If you press Enter without specifying any information, all existing dataset profiles are displayed, which usually results in too much data.

Dataset profile is the most important field on the Data set Selection panel. If you know the name of the profile you are looking for, you can specify the **Exact** specification here. You can also specify an **EGN mask** that covers the profile, **Match** the name of a data set to the profile that covers it, or look for all matching profiles (**Any match**). For example:

1. Type `SYS1.**` and empty all other fields except **1** for **EGN mask**.

   Remember that in EGN, the name pattern `SYS1.*` (with one asterisk) matches any name with a single qualifier following `SYS1`. If you specify `SYS1.**` (with two asterisks), this value matches any name with any number of qualifiers behind `SYS1`. For example, you can look for any profile that begins with `SYS` by using a filter like `SYS*.**`.

2. Press Enter.

   A panel opens showing all the dataset profiles starting with `SYS1`, for example. This panel is like the panel shown in Figure 13 on page 18.

```
zSecure Admin+Audit for RACF DATASET Overview          1 s elapsed, 0.2 s CPU
Command ===> _____________________________________________ Scroll===> CSR_
like SYS1.**                                    8 Apr 2005 00:25
   Profile key                                 Type    UACC    Owner    S/F W
__ SYS1.ACDS                                   GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.BRODCAST                               GENERIC UPDATE_ SYSPROG_ __R _
__ SYS1.CMDLIB                                 GENERIC READ___ SYSPROG_ U_R _
__ SYS1.COMMDS                                 GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.C#M.LINKLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.CSSLIB                                 GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DFQLLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DGTLLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.DUMP*.**                               GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.HASPACE                                GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.IBM.PARMLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.IBM.PROCLIB                            GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ICEDGTL                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ICEISPL                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ISAMLPA                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.ISP*                                   GENERIC NONE___ SYSPROG_ __R _
__ SYS1.JESCKPT*.**                            GENERIC NONE___ SYSPROG_ R_R _
__ SYS1.LINKLIB                                GENERIC NONE___ SYSPROG_ U_R _
__ SYS1.LOCAL.LINKLIB                          GENERIC READ___ SYSPROG_ U_R _
__ SYS1.LOCAL.VTAMLIB                          GENERIC READ___ SYSPROG_ U_R
```

Figure 13. Dataset profile

Other selection criteria are available:

- Best match result
  1. To exit the data set overview and return to the Data set Selection panel, press PF3.
  2. In the **Dataset profile** field, type `SYS1.DUMP00` and select **3** for **Match**.
  3. Press Enter.

     A panel similar to the one shown in Figure 14 opens showing the profile best matching `SYS1.DUMP00`.

```
zSecure Admin+Audit for RACF DATASET Overview            1 s elapsed, 0.4 s CPU
 Command ===> _____________________________________________ Scroll===> CSR_
 exact match SYS1.DUMP00                        8 Apr 2005 00:25
   Profile key                                 Type    UACC    Owner    S/F W
 __ SYS1.DUMP*.**                              GENERIC NONE___ SYSPROG_ R_R _
 ****************************** BOTTOM OF DATA ********************************
```

Figure 14. Best match result

- Any match result
  1. To exit the data set overview and return to the Data set Selection Panel, press PF3.
  2. In the **Dataset profile** field, leave the `SYS1.DUMP00` value, and select **4** for **Any match**.
  3. Press Enter.

     A panel similar to the one shown in Figure 15 on page 19 opens showing all profiles matching `SYS1.DUMP00`. The best-fitting profile is shown in the top line. In addition, less specific profiles are shown that could match the resource, if the top profile was deleted.

```
zSecure Admin+Audit for RACF RACF DATASET Overview        1 s elapsed, 0.5 s CPU
 Command ===> _____________________________________________ Scroll===> CSR_
 any match SYS1.DUMP00                              8 Apr 2005 00:25
    Profile key                                     Type    UACC    Owner    S/F W
 __ SYS1.DUMP*.**                                   GENERIC NONE___ SYSPROG_ R_R _
 __ SYS1.*.**                                       GENERIC NONE___ SYSPROG_ U_R _
 ****************************** BOTTOM OF DATA ********************************
```

Figure 15. Any match result

- In addition to the mask and matching selection options, other selection criteria are available. These can be very useful when you are searching for specific type of dataset profiles. For example:
  1. Press PF3 to return to the Data set Selection panel.
  2. Type **/** in the **Profile** fields in the **Additional selection criteria** area.

     This action opens another panel so that you can specify additional selection criteria.

Finding profiles in warning mode

Warning mode means that all accesses are permitted, but a warning message is issued if the access normally results in a violation. Warning mode is usually a temporary measure because it permits any action on data sets covered by the profile. To list all the profiles that are in warning mode, complete the following steps:

1. Make sure that there is a **/** next to the **Warning mode** field and remove the selection (**/**) next to the **No warning** field.
2. Press Enter.

   The display lists all profiles that are in warning mode. Your search can be more specific, such as `HLQ=PAYROLL` and Warn mode.
3. Press PF3 to return to the Data set Selection panel. Then try entering `PROD.**` (or something meaningful for your installation) in the **Dataset profile** field and **2** (READ) in the **UACC** or **ID**(*) field. (This is found in the same panel where earlier you selected the warning mode.)

   Remember to reapply the **/** next to the **No warning** field in the inclusion criteria section.
4. Press Enter.

   This action produces a list of production data sets that any user can read.
5. Press PF11.

   This action shows additional fields such as the **ERASE** (**E**) field. If a profile has the RACF ERASE ON SCRATCH (EOS) attribute, then any dataset protected by the profile is physically erased to ensure data confidentiality when it is deleted.
6. Use the **S** line command or move the cursor to the beginning of any displayed data line to obtain the details for that particular profile.

   Note: Remember that many lines in the displays can be expanded. Enter an **S** in the first field of the line or position the cursor in the first field and press Enter.

Displaying discrete profiles

To display discrete profiles, complete the following steps:

1. Return to the Data set Selection panel.
2. Erase the **Dataset profile** field.

3. Type a **/** before **Profile fields** in the **Additional selection criteria** section. Then press Enter.
4. Make sure that nothing is filled in for the **UACC at least** field.
5. Check that there is a **/** in the **Discrete** selection field in the Data set Selection panel.
6. Remove the **/** from the **Generic selection** field, and leave all other selection criteria as they are.
7. Press Enter.

   This action produces a list of all existing discrete dataset profiles.

Tip: Remember that the zSecure Audit for RACF uses the *AND* function when you specify multiple properties.

Displaying the access control list (ACL)

The next steps open a list of dataset profiles from which you select a specific profile to obtain detailed information, like the access control list (ACL), as well as information related to each entry in the ACL and some of its characteristics. Select a dataset profile that you know has multiple, complex usage permissions in your RACF database. You can use wildcard characters to specify the selection criteria. The following examples select dataset profiles with a name pattern matching `SYS1.**` as an example, but use one that is appropriate for your installation. In the Data set Selection panel, complete the following steps:

1. Type the profile name in the **Dataset profile** field.
2. Type a **/** next to the **Enable full ACL** field in the **Output/run options** section.
3. Press Enter to open the list of all matching profiles.
4. Select the most complex dataset profile from the list, based on your knowledge.
5. Type an **S** line command for that line. Then press Enter.

```
zSecure Admin+Audit for RACF DATASET Overview                    Line 1 of 33
Command ===> ____________________________________________________ Scroll===> PAGE
any matching SYS1.PROCLIB                      6 Oct 2009 03:31


_ Identification                                                        SYS1
  Profile name                 SYS1.PROCLIB
  Type                         GENERIC
  Volume serial list
_ Effective first qualifier    SYS1                          MOST SUPERIOR GRO
_ Owner                        SYSPROG                       SYSTEM PROGRAMMIN
  Installation data            ____________________________________________

  User     Access  ACL id   When               RI Name                DfltGrp
_ -group-  ALTER   SYSPROG  ________ __________
_ -group-  READ    SYS1     ________ __________

  Safeguards                           Other permissions
  Erase on scratch             No      Allow all accesses    WARNING No
  Audit access success/failures U R    Universal access authority    READ
  Global audit success/failures ___    Resource level                 0
  User to notify of violation  ________
  Days protection provided #   _____
```

Figure 16. Normal ACL

In Figure 16, you can see that in this case the ACL contains only group entries.

Access control list formats

In RACF, you can easily have multiple, inconsistent access permissions for a resource. For example, you can have read permission through a group to data set *XXX* and you can also belong to another group that has update permission to *XXX*. RACF grants the user the highest access level available in such multiple permissions. In our example, the user would have update authority.

Additionally, a specific user permit takes precedence. RACF resolves multiple access permissions to determine the operative permission. zSecure Admin and Audit can display resolved permissions, or it can display exploded permissions, showing all permissions that exist. The resolved permission is the only one that counts when granting access to a resource, but an exploded list is vital when trying to determine why a user has a certain level of access to a resource. By default, zSecure Admin and Audit displays the access control list exactly as RACF would display it, but ordered by groupid or userid and including the userid, programmer name, and installation data.

To show a list of all users connected to these permitted groups and any user who has permission by other reasons, type **ACL EXPLODE** or **ACL X** in the command line. This command opens an exploded list (which might be more than one line per user) showing those users with access to this profile. The detailed display indicates which access control list entries provide what level of access for the users.

All users with access to the data set are displayed, along with their connect group; see Figure 17. Even access through system-wide and group-OPERATIONS is indicated.

```
zSecure Admin+Audit for RACF DATASET Overview                    Line 1 of 63
 Command ===> ____________________________________________________ Scroll===> PAGE
 any matching SYS1.PROCLIB                        6 Oct 2009 03:31


 _ Identification                                                      SYS1
   Profile name                 SYS1.PROCLIB
   Type                         GENERIC
   Volume serial list
 _ Effective first qualifier    SYS1                          MOST SUPERIOR GRO
 _ Owner                        SYSPROG                       SYSTEM PROGRAMMIN
   Installation data            ____________________________________________

  User     Access  ACL id   When              RI Name                  DfltGrp
 _ C#MBERT  ALTER   SYSPROG                      BERT JOHNSON          SYSPROG
 _ C#MBERT  READ    SYS1                        BERT JOHNSON          SYSPROG
 _ CRMBFT1  ALTER-O - oper -                    FRANK TRATORRIA SPEC. SYSPROG
 _ CRMBFT1  ALTER   SYSPROG                     FRANK TRATORRIA SPEC. SYSPROG
 _ DEPT2    READ    SYS1                        USR =QA OW=DEPT       USR =QA CN
 _ DFHSM    READ    SYS1
```

Figure 17. Exploded ACL

In Figure 17, the line:

```
_ CRMBFT1  ALTER-O - oper -                    FRANK TRATORRIA SPEC. SYSPROG
```

shows an example where access is granted because the user has OPERATIONS authority. The following line shows that the user DEPT2 is connected to group SYS1 and has READ access on the dataset profile.

```
DEPT2    READ    SYS1                        USR =QA OW=DEPT       USR =QA CN
```

A user can have multiple access rights to the same dataset profile through different paths. A line is shown for each of a user's access rights and group connections. For

example, as Figure 17 on page 21 shows, user C#MBERT is displayed in two different lines because this user is connected to group SYS1 and has READ access and this user is also connected to group SYSPROG and has ALTER access.

Tip: Avoid using the EXPLODE option. The SORT option is best for general use.

To show only the highest level that a user has, complete the following steps:

1. Type **ACL RESOLVE (R)** in the command line.

   A list is displayed showing only one entry for each user, indicating exactly what access each user has. Be aware, however, that access by means of the system-wide and group-OPERATIONS attribute is not included in the resolved overview display.
2. Type **ACL EFFECTIVE (F)** in the command line.

   A list is displayed showing only one entry for each user, indicating exactly what access each user has. The list, however, also includes users who have access because they possess the OPERATIONS attribute.
3. Type **ACL SORT ACCESS** in the command line.

   A list is displayed showing the access control list by descending access level and for each access level by userid. See Figure 18.

```
zSecure Admin+Audit for RACF DATASET Overview                    Line 1 of 44
Command ===>  ____________________________________________ Scroll===> CSR
like SYS1.                                  ** 8 Apr 2005 12:17
 Identification                                                DEMO
 Profile name                 SYS1.PROCLIB
Type                         GENERIC
   Volume serial list
 _ Effective first qualifier    SYS1                       MOST SUPERIOR GRO
 _ Owner                        SYSPROG                    SYSTEM PROGRAMMIN
   Installation data            ____________________________________________
   User     Access  ACL id   When            RI  Name                 InstData
 _ C#MBERT  ALTER   SYSPROG                      BERT JOHNSON
 _ C#MBMR1  ALTER   SYSPROG                      M RONTEL             AAAAAAAAAA
 _ R##SLIN  ALTER   SYSPROG                      BERT JOHNSON SPEC.
 _ SYSPSTC  ALTER   SYSPROG                      STC USER SYSPROG
 _ CNRUNL   READ    SYS1                        JUST A USER TO BE US
 _ DEPT     READ    SYS1                        USR =QA OW=SYS1       USR =QA CN
 _ DEPT1    READ    SYS1                        USR =QA OW=DEPT       USR =QA CN
 _ DEPT2    READ    SYS1                        USR =QA OW=DEPT       USR =QA CN
 _ DFHSM    READ    SYS1
```

Figure 18. Effective ACL

The **ACL EFFECTIVE** command shows you the effective access that individual users have, including access through system and group operations. If you also want to include ownership rights through owner, qualifier, or group-SPECIAL, you can toggle this on and off by using the commands **ACL SCOPE** and **ACL NOSCOPE**. If you want to see access rights and ownership rights separately but still resolved, you can specify **ACL TRUST** instead of **ACL EFFECTIVE**.

Tip: To print a display, go to the command line and type **PRT**. This command prints the current display, including the full report width, which can be wider than the screen of the typical user, and the higher-level information leading to this panel. The printed output is placed in your ISPF LIST data set. When you exit ISPF, remember to print this data set. If you want to print the ISPF LIST data set without leaving ISPF, enter **LIST** in the command line and select your printing options in the resulting panel.

Changing the access list display settings

This brief discussion of resolve and explode is an important feature for you to remember. You can change the layout of the access control list in these ways:

- Use **Option 5** from the Setup panel to access the Setup View panel.
- Type **SET** in the Command area of an access control list display.
- Type an **ACL RESOLVE**, **ACL EXPLODE**, or **ACL EFFECTIVE** command in the Command area of an access control list display.

The first two methods remember the new mode for future use. The last method changes only the current display.

To change the access list display settings from the Setup View panel, complete the following steps:

1. Type **SETUP VIEW** in the command line to open the Setup View panel shown in Figure 19.

```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                         zSecure Admin+Audit for RACF - Setup - View
Command ===> ____________________________________________________________________

Access list format . . . . 2  1. No       3. Explode  5. Effective
                              2. Sort     4. Resolve

ACL/Connect sort . . . . . 2  1. Id       2. User     3. Access

Show OS specific options   /  z/OS        _  z/VM

/  Add user/group info to view
   (Selecting this will use some additional storage - normally on )
/  Add summary to RA displays for multiple RACF sources (normally on)
_  Add connect date and owner to RA.U connect group section

Select view
3  1. View only profiles you are allowed to change (administrator view)
   2. View only profiles you are allowed to change or list
   3. View all profiles (normal view)
```

Figure 19. Setup View panel

2. In the **Access list format** field, specify option **5**.
3. Press PF3 to ACCEPT the new value. The value is in effect the next time you do a query. From now on, you see only one line for each user. This represents the effective access level for each user.

The resolve or explode display level you set is in effect until you change it. The Setup View panel is one of the Setup panels. You can also access it through the Setup menus, which are described next.

To change the access list display settings from the Setup panel, complete the following steps:

1. Return to the Main menu using PF3.
2. Select option **SE** (Setup).
3. Select option **5** (View).

Tip: Instead of typing these commands, you can also type **=SE.5** in the command line to go immediately to the Setup View panel.

4. To change the Access control list format back to **SORT**, type **2** in the **Access list format** field.

   The Sort format is the most appropriate format for general use.
5. Press PF3 to exit the panel.

Using the Access command

Note
This command is applicable only for the zSecure Admin product.

You can use the Access function **RA.1** to see the data sets or resources (and by means of which RACF profile) that a specific user or group has access to. By typing a userid and a resource class and a data set name, general resource name, or RACF profile name, the Access function answers the question of which profile covers the resource and what the resulting access is for the user.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                zSecure Admin - RACF - Access Check
Command ===> ____________________________________________________________________

Id  . . . . . . . . IBMUSER_

Specify profile for Access Check
 Class  . . . . . . DATASET_   (DATASET or class)
 Profile  . . . . . SYS1.LOADLIB_____________________________ (EGN mask)
```

Figure 20. Access check entry panel

To use the Access function, complete the following steps:

1. In the **Id** field, type the userid or group id.
2. Specify the resource class (*dataset* or a general resource class name) and the data set name, resource name, or profile name in the **Profile** field.
3. Press Enter.

   The Access check detail panel illustrated in Figure 21 opens to show you the access level that RACF grants to this ID, and where the access is coming from.

```
   Menu  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 BROWSE    IBMUSER.CKRACF1.SDEMO.CKXOUT               Line 00000000 Col 001 080
 Command ===> ____________________________________________ Scroll ===> CSR_
******************************** Top of Data ********************************
CKGRACF ACCESS IBMUSER DATASET SYS1.LOADLIB
CKG582I 00 IBMUSER has ALTER access to DATASET SYS1.LOADLIB
           profile DATASET SYS1.**
******************************* Bottom of Data *******************************
```

Figure 21. Access check detail panel

Managing access rights

There are several ways to administer the access control list of a dataset profile:

- Issue line command **PE** (permit) in the Data set profile Overview panel.
- Use a **C** (copy), **D** (delete), **I** (insert), **R** (repeat) or **S** (modify) line command in the dataset profile detail panel.

- To change a value, type over the current value in the access control list.

  When you change the values, **Permit** and **Permit Delete** commands are generated to add the new value and remove the value that was overwritten.

  If you do not want to execute the **Permit Delete** command, remove it from the command confirmation panel before you press Enter. Press Enter again in the next panel (zSecure Admin – Confirm command) to process your **Permit** command. Do not execute the RACF commands at this time.

Reporting digital certificates

Many companies use digital certificates to authenticate their authorized users. You can report on digital certificates that are currently stored in your RACF database.

To report on digital certificates, complete the following steps:

1. Press PF3 until you are on the Main menu.
2. Select option **DIGTCERT (RA.5)** from the RA panel to open the DIGTCERT panel shown in Figure 22.

```
   Menu         Options       Info    Commands     Setup           Startpanel
--------------------------------------------------------------------------------
                    zSecure Suite - RACF - DIGTCERT
Command ===> ____________________________________________________________________

Show certificates that fit all of the following criteria
Owner  . . . . . . . . . .  _  Personal  ________  _  Site   _  Certauth
Start validity . . . . . __  ___________  (operator: > >= < <= = >< ¬= )
End validity . . . . . . __  ___________  (date: yyyy-mm-dd/ddMMMyyyy/
                                            TODAY/TODAY-nn/NEVER)

Trust  . . . . . . . . . .  _  1. TRUST    2. NOTRUST  3. HIGHTRUST   4. Ignore

Output/run options
_  Print format          Customize title     Send as e-mail
     Background run  /  Full page form   /  Sort differently  /  Narrow print
```

Figure 22.

To use this panel to report all digital certificates stored in the RACF database, leave all fields blank and press Enter. You can use this functionality to quickly identify digital certificates that are expired or due to expire.

To find out which digital certificates are due to expire soon, complete the following steps:

1. Specify **< TODAY+30** in the **End validity** field. This command reports only the digital certificates that are already expired or due to expire in the next 30 days.
2. Using the **Trust** field, you can restrict the output to contain only the certificates that are currently trusted (**option 1**), not trusted (**option 2**), or highly trusted (**option 3**).
3. Finally, using the **Owner** field, you can select certificates for one or more user IDs (PERSONAL), all certificate authority certificates (CERTAUTH), or all site certificates (SITE).

   For PERSONAL certificates, you can optionally use filters to select certificates for multiple user IDs. You can use the percent symbol (%) to select one character and you can use the asterisk symbol (*) to select zero or more characters.

You cannot generate RACDCERT commands from this panel.

Comparing users

Often users ask a question such as, "Why doesn't this function work for me, while it does for my neighbor? I thought we were supposed to have the same access to that product?" You can use zSecure Admin and zSecure Audit for RACF for quick comparison of the access and connect status for up to four users.

To compare the access and connect status of users, complete the following steps:

1. Press PF3 until you are on the Main menu.
2. From the Main menu, select option **REPORTS (RA.3)** from the RA panel. Select option **G Compare users** from the resulting to open the Compare users panel shown in Figure 23.

```
 Menu  Options  Info  Commands     Setup
 ------------------------------------------------------------------------------
         zSecure Admin+Audit for RACF - Reports - Compare users
 Command ===>

Enter up to 4 userids to compare access and/or connects
 Userid  . . . . ________    ________    ________    ________

Select report(s)
/  Compare access through user-specific permits
     _  Include group permits
/  Compare connects
```

Figure 23. Compare users panel

On this panel, you can specify up to four users, and the exact comparisons that you want to do. Up to two reports are generated: one for permits, and one for group connects.

The Permit report is presented in three layers:

1. The classes for which permits are present with the highest access of each user to any profile in that class.
2. The profiles in the selected class, once again those with the highest access
3. A list with all permits for the selected users on a specific profile.

This detailed display also shows the information from the higher layers for this one specific entry, as shown in Figure 24.

```
Compare PERMITs for users                                        Line 1 of 2
Command ===> ____________________________________________ Scroll===> CSR
                                          10 Oct 2006 00:07
   Class    Profiles C#MBDV1 C#MBDV2
   DATASET        32 ALTER   ALTER
   Profile key                            C#MBDV1 C#MBDV2
   C#MA.D.HLLDV1.PADS.**                  READ    ALTER
   Scope of Access  Via      When
__ C#MBDV1  READ    CR#BDV1  PROGRAM  CKRCARLA
__ C#MBDV2  ALTER   CR#BDV2
****************************** Bottom of Data ********************************
```

Figure 24. Compare permits detail panel

The connect report shows a matrix of all groups to which at least one of the users is connected, as shown in Figure 25 on page 27:

```
Compare CONNECTs for users                                        Line 1 of 6
Command ===> _____________________________________________ Scroll===> CSR
                                              10 Oct 2006 00:07
   Group    C#MBDV1  C#MBDV2
__ C#MARACF No       Yes
__ C#MB     Yes      Yes
__ C#MBREAD Yes      Yes
__ C#MBZDEV Yes      Yes
__ C#MCKG   No       Yes
__ C#MGRACF Yes      Yes
****************************** Bottom of Data ********************************
```

Figure 25. Compare connects matrix

Chapter 3. Managing users and profiles

Note
This section is applicable only for the zSecure Admin product.

Using zSecure Admin, you can change RACF data in the following ways:

- You can change a value by typing over the existing value in a field on a profile display.
- You can use line commands in a profile display, like **C** (Copy), **D** (Delete), **R** (Recreate), **L** (list), and **SE** (Segments).
- You can use the Mass Update panels.
- You can submit foreground or background RACF commands that are automatically generated by various Report and Verify functions.
- You can use the distributed functions, described in Chapter 4, "Using distributed and scoped administration functions," on page 41.

The first three methods (typing over a value, line commands, and Mass Update) are controlled by the Confirm panel in the Setup panel. See "Generating and confirming RACF commands." The Confirm panel enables or disables the Overtype function and determines what verification is required before running a RACF command that changes the database. You can set this confirmation control as you desire. However, until you are quite familiar with routine product usage, use the ALL or PASSWORDS setting.

Generating and confirming RACF commands

To generate and confirm RACF commands, complete the following steps:

1. Select option **SE** (Setup).
2. Select **option 4** (Confirm) to open the Confirm panel showing the current settings, as shown in Figure 26 on page 30.

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
             zSecure Admin+Audit for RACF - Setup - Confirm
Command ===> ____________________________________________________________

Action on command . . 2  1. Queue    2. Execute  3. Not allowed
                      _ Execute display commands (for option 1 only)
Confirmation  . . . . 4  1. None     2. Deletes  3. Passwords      4. All
Command Routing . . . 3  1. Ask      2. Normal   3. Local only

Command generation
Enter "/" to select option(s)
/  Overtype fields in panels
/  Change generated commands
/  Specify start/end date
/  Generate SETROPTS REFRESH commands
   /  Issue prompt before generating SETROPTS REFRESH commands

Commands to generate
/  RACF commands
/  CKGRACF commands
/  CKGRACF ASK for later execution
/  CKGRACF REQUEST for later execution
_  CKGRACF WITHDRAW queued commands
_  CKGRACF RDELETE queued commands
```

Figure 26. Confirm panel

3. Set the **Action on command** field to **2** (Execute).
4. Set the **Confirmation** field to **4** (All).
5. Set the **Command Routing** field to **3** (Local only).
6. Set **Overtype fields in panels** to **/**.

   This option is used in the following examples. Leave all other settings as they are, especially in the **Commands to generate** section.

   Tip: You can also switch modifiable fields on and off by entering the **MODIFY** command (or just **M**) in the command line of any profile display.
7. Press PF3 to accept the changed parameters.
8. Press PF3 again to return to the Main menu.

   Tip: You can always reach the Confirm panel by typing **SETUP CONFIRM** or **=SE.4** in the command line of any panel.

If you want to manage the RACF database from zSecure Admin using your user ID, you must have the correct authority for the RACF database. The required authority is usually RACF SPECIAL, although group-SPECIAL might serve if you are selective about attempted changes. An alternative is to use the CKGRACF program, which has its own security scheme, instead of SPECIAL authority; see "Using CKG scope for group administration" on page 42.

Performing a mass update

To perform a mass update, complete the following steps:

1. Select option **RA** (RACF Administration).
2. Select **option 4** (MASS UPDATE) to open the Mass update panel shown in Figure 27 on page 31.

Using Options **0** to **5** from the Mass Update panel, you can manage profiles at the entity level, like user and group. For example, when you delete a user, you delete not only the user profile, but also all profiles related to the original userid.

Additionally, the PERMITS and CONNECTS are removed, as well as the ALIAS in the master catalog. All information is managed at one time.

```
   Menu   Options   Info   Commands   Setup    StartPanel
------------------------------------------------------------------------------
           zSecure Admin+Audit for RACF - RACF - Mass update
Option  ===> ____________________________________________________________

0    Copy user       Copy existing user(s) to new user(s)
1    Copy group      Copy existing group(s) to new group(s)
2    Copy dataset    Copy dataset profile(s) to another high level qualifier
3    Copy resource   Copy general resource profile(s) to another class
4    Delete user     Delete user(s)
5    Delete group    Delete group(s)
6    Recreate user   Recreate user(s)
7    Recreate grp    Recreate group(s)
8    Recreate ds     Recreate data set profile(s)
9    Recreate res    Recreate general resource profile(s)
C    Copy CICS       Copy CICS prefixed profile(s) or member(s)


Product/release: IBM Security zSecure Admin and Audit for RACF 1.9.0
```

Figure 27. Mass update

The Mass Update panels provide many functions that are difficult to do with regular RACF commands. Some especially important points are highlighted.

Copying a user

You can clone an existing user using the **Copy user** option (Option 0). Besides copying the user profile, this command also copies the permits and connects of the model user. zSecure Admin also provides the option to create a user ALIAS in the master catalog.

To copy a user, complete the following steps:

1. Select option **0** (Copy user) from the Mass Update panel to open the User Multiple copy panel, shown in Figure 28 on page 32.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - RACF - User Multiple copy
Command ===> ____________________________________________________________

Create new user(s) like existing user(s):

_ Specify password phrases

Model
User     New user Password Name                 Owner    Dfltgrp  Data
IBMUSER_ NEWUSER1 PSWD1___ PERSON_1____________ C#MB____ ________ ____________
=_______ NEWUSER2 PSWD2___ PERSON_2____________ =_______ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________
________ ________ ________ ____________________ ________ ________ ____________


Enter = to copy value from preceding line, leave blank to copy from model.
Press ENTER to specify optional parameters.
```

Figure 28. User multiple copy panel

You can clone up to 10 users at a time, but for the evaluation, complete only the first line.

2. If you want to specify password phrases, type **/** in the **Specify password phrases** selection field.

   After you press Enter, a follow-up panel is displayed so that you can enter the password phrases for the user IDs. You cannot use the protected option if you specify password phrases.
3. Specify the model user: type your userid, the new userid, the name, and a password.

   Tip: You can use * in the password column to make the new user protected.
4. Press Enter.
5. Press Enter in the next panel.

   This panel provides the option to perform the following functions for the new user:

   - Omit or add additional group connections.
   - Copy user data.
   - Revoke the new user or users.
   - Create one or more catalog aliases.
   - Copy one or more data set and general resource profiles.
   - Copy one or more members of RACF variables (RACFVARS) for the new user.

   Any command necessary to create the new user from the model profile is generated. After a few moments, a PDF edit panel is displayed with a complete set of RACF commands. You can scroll using PF8 and PF7 to go forward and backward and make changes if applicable.
6. Press PF3 to quit the editor.
7. Press PF3 to skip the Result panel.

   The Result panel is described in Chapter 6, “Reporting,” on page 57.
8. Press PF3 until you are back on the Mass Update panel.

If the commands had been executed, the new user would have been defined exactly as the model user. You can also keep the generated commands in a data set for delayed execution.

Deleting a user with all references

You can completely remove a user with option **RA.4.4** (Delete user), which is a tedious operation if done with regular RACF commands. Completely removing a user removes the userid from all access control lists and owner and notify fields, in addition to removing the profile. If you have allocated a CKFREEZE file, this operation also deletes the catalog alias and existing data sets for the user if you select the required options. See Figure 43 on page 49.

Recreating a profile

You can recreate profiles with options **RA.4.6** through **RA.4.9** based on data in the unloaded RACF data set or a backup copy of the RACF database itself. This action can be used to repair profiles damaged by errors or deleted by mistake.

Merging profiles

There are several other interesting features for merging RACF databases or comparing RACF databases. Merging is done by making an unloaded copy of one RACF database and using it to change and add profiles in another RACF database. For confirming or editing, all RACF commands to be used for merging the RACF profiles are listed. This command list is a comparison of the relevant profiles in the RACF and unloaded data set. A complete merge is more complex than described here and is fully documented in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

Displaying redundant profiles

It is a good practice to regularly take a close look at the dataset profiles defined in your RACF database. To determine which dataset profiles are, or might be, obsolete, you can use the **RA.3.3** function. This function opens the Reports Redundant panel shown in Figure 29.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
          zSecure Admin+Audit for RACF - RACF - Reports REDUNDANT
Command ===> ____________________________________________________________

Show profiles that fit all of the following criteria:
Profile pattern . . _____________________________________________ (EGN mask)
High level qual . . SYSA____      (qualifier or EGN mask; reduces time)
Complex . . . . . . ________      (complex name or filter)

Enter "/" to select option(s)
_  Show data sets covered by each profile
   _  Including data sets on scratch tapes

_  Output in print format
   _  Start each user or group on a new page

_  Remove redundant profiles
```

Figure 29. Reports Redundant panel

In the panel shown in Figure 29, you can specify which dataset profiles or High Level Qualifier (HLQ) you want to include in the report. If these fields are left

blank, all dataset profiles are automatically processed. You can also specify whether you want to include the names of all data sets that are covered by the dataset profiles in the report.

The Report Redundant function compares dataset profile security definitions such as UACC, access control list, audit settings, and erase on scratch setting, to those of the next less specific generic dataset profile.

When the security settings are not significantly different, the profile is reported as `-redundant-`. This value indicates that when this more specific dataset profile is deleted, the protection of the data sets is automatically taken over by the less specific generic dataset profile (indicated as `-candidate-`) without causing any changes in the security definitions for the corresponding data sets.

```
Redundancy analysis of dataset profiles                          Line 61 of 445
 Command ===> ____________________________________________________ Scroll===> CSR_
                                          8 Apr 2005 15:57
    Complex  Timestamp         Profiles Non-redundant
    DEMO      8 Apr 2005 15:57      445           364
    Qual     Profiles Non-redundant
    SYSA          445           364
    Type    Volume Profile name                                   First reason
__ GENERIC        SYSA.D.CCW*.**                                  - candidate -
__ GENERIC        SYSA.D.CCW*.**                                  Extra group
__ GENERIC        SYSA.D.CCWSCH.**                                User privileged
__ GENERIC        SYSA.D.CCW300.*.BASELIST                        - redundant -
__ GENERIC        SYSA.D.CCW300.**                                - candidate -
__ GENERIC        SYSA.D.CCW300.**                                Access
__ GENERIC        SYSA.D.CCW301.**                                Access
__ GENERIC        SYSA.D.CCW302.**                                Extra group
__ GENERIC        SYSA.D.CCW303.**                                Access
__ GENERIC        SYSA.D.CCW305*.**                               Access
__ GENERIC        SYSA.D.CCW310.**                                Access
__ GENERIC        SYSA.D.CCW311.**                                Access
__ GENERIC        SYSA.D.CCW312.**                                Extra group
```

Figure 30. Report redundant details panel

In Figure 30, the following line shows an example of a profile that can take over protection of data sets when the profile marked as `-redundant-` is deleted.

```
__ GENERIC        SYSA.D.CCW*.**                                  - candidate -
```

The following line shows an example of a profile that can be deleted because the security settings are similar to those of the candidate profile that automatically takes over protection.

```
__ GENERIC        SYSA.D.CCW300.*.BASELIST                        - redundant -
```

The output of the report on redundancy is an overview of all dataset profiles with an indicator in the column headed by **First reason**. The first reason column can contain any of the following values:

-redundant-
: With the current security definitions, this profile is not required and can be removed. Protection of the data sets covered by the redundant profile is automatically taken over by a less specific dataset profile (marked with `-candidate-`) that is displayed in the same report somewhere above the profile being reported as a `-redundant-` profile.

-candidate-
This profile takes over the protection of data sets that are currently protected by a more specific generic dataset profile, when the latter is deleted.

reason This field provides a textual description to indicate why this profile differs significantly from the less specific generic dataset profile and therefore is not considered redundant. Sample reason values are: `Extra group`, `User privileged`, and `Access`. When multiple differences exist, only the first reason is reported.

The report on redundancy can help you determine which dataset profiles have become obsolete over time in the current RACF database.

Optionally, you can generate RACF commands to delete the profiles that are reported as `-redundant-`. Be aware, however, that you might not want to delete all profiles marked `-redundant-`. It is possible that a mistake was made at the time this dataset profile was defined; that is, you or another RACF administrator has forgotten to activate erase on scratch or change the audit setting as intended.

Tip: The redundancy analysis can be useful to indicate any mistakes that you might have made during dataset profile definition.

Displaying data structure

Another very useful report when managing your RACF database is the Group tree report. In native RACF, the only way to display the RACF database structure is by processing the Group tree report using the DSMON utility. For each requested group, this report lists all of its subgroups, all of the subgroups' subgroups, and so on. In addition, the report lists the owner of each group listed in the report, if the owner is not the superior group. Only users that have the AUDITOR attribute can use the DSMON utility. However, no AUDITOR attribute is required to process the Group tree report.

In zSecure Admin, there is a standard function for processing a Group tree report. The group tree visualizes the group tree structure, similarly to how a browser displays the contents of your hard disk or network drive.

To process the Group tree report, complete the following steps:

1. Select option **RA** (RACF Administration).
2. Select option **3.8** (Group tree) to open the Reports Group tree panel shown in Figure 31 on page 36.

```
Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
         zSecure Admin+Audit for RACF - RACF - Reports Group tree
Command ===> ____________________________________________________ _ start panel

Show structured group tree display:
Group id  . . . . . ________     (group profile key or filter)
Start at  . . . . . ________     (group or filter, show only groups below)
Scope of  . . . . . ________     (group special, show only groups in scope)
Exclude . . . . . . ________     (group or filter)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to include data in output
/  Installation data
/  Users/Subgroups

Enter "/" to select option
_  Output in print format


'Start at' is only allowed with an unload as data source, not a live database
```

Figure 31. Group tree selection panel

You display only a particular branch of the RACF group tree by entering a group name (or filter) in the **Start at** field. This option is permitted only when running with an unloaded data source. If all fields are left blank, the entire group tree for your RACF database is displayed.

Optionally, you can indicate that you want to include the Installation data in the group tree report by entering a **/** in front of **Installation data**. The Installation data is generally used to store the group description.

Furthermore, to include detailed information regarding subgroups and connected users in a detail level panel, type a **/** in front of the **Users/Subgroups** field.

3. Press Enter to open the Group tree report panel, which shows all groups in your current RACF database. See Figure 32.

```
zSecure Admin+Audit for RACF GROUP TREE DISPLAY       1 s elapsed, 0.5 s CPU
 Command ===> ____________________________________________ Scroll===> CSR_
                                          8 Apr 2005 16:57
    Complex  Groups
    DEMO        267
    Group structure                    Lvl Subgrp Connct SupGroup Owner    X
__   SYS1                                1     19     11 ........ IBMUSER_ X
__   BOOKS                               2      0      0 SYS1____ SYS1____
__    C#                                 2      7      1 SYS1____ SYS1____
__     C#ADMIN                           3      0     10 CR______ CR______
__     C#M                               3      9      2 CR______ CR______
__      C#MBCCW                          4      0      5 C#M_____ C#M_____
__      C#MCKG                           4      0     33 C#M_____ C#M_____
__      C#MPC2E                          4      0      9 C#M_____ C#M_____
__      C#MPC4R                          4      0      0 C#M_____ C#M_____
__      C#MQ                             4     23      0 C#M_____ C#M_____
__       C#MQA                           5      8    241 C#MQ____ C#MQ____
__        C#MBQAHW                       6      2      1 C#MQA___ C#MBWTK_ X
__         C#MBQAHU                      7      0      0 C#MBQAHW C#MBQAHW
__         C#MBQAH2                      7      0      1 C#MBQAHW C#MBWTK_ X
__        C#MBQALU                       6      0      1 C#MQA___ C#MQA___
__        C#MBQAMC                       6      0     12 C#MQA___ C#MQA___
__        C#MQA#HI                       6      0      0 C#MQA___ C#MQA___
__        C#MQAT#1                       6      0      0 C#MQA___ R##SLIN_ X
```

Figure 32. Group tree report panel

In the Group tree report panel shown in Figure 32 on page 36, the X in the X column indicates a scope break for group special users because owner is not equal to the superior group.

4. If you requested Installation data, press PF11 to review the information.
5. Press PF8 a few times to look at more parts of the group tree structure.
6. If detailed information was included in the report and you want to view it, enter the **S** line command in front of a group to open the Group tree report detail panel shown in Figure 33.

```
zSecure Admin+Audit for RACF RACF GROUP TREE DISPLAY            Line 1 of 11
Command ===> _____________________________________________ Scroll===> CSR_
                                              8 Apr 2005 16:58
   Group structure                         Lvl Subgrp Connct SupGroup Owner    X
       C#MCDEMO                              4      1      5 C#MC     C#MC
  User     Auth    R SOA AG Uacc    Name                 InstData
_ C#MCCW1  USE      _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW2  USE      _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW3  USE      _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW4  USE      _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
_ C#MCCW5  USE      _ ___ __ NONE    /CCW + VIEW          WORKSHOP HANDS-ON USER
   SubGroup
_ C#MCDEM2
```

Figure 33. Group tree report detail panel

Running SETROPTS reports and viewing class settings

To take a close look at or administer the current system-wide RACF options or the Class Descriptor Table (CDT), using zSecure Admin, you can use either the RA.S or AU.S functions. This section provides information about the RA.S function. Details on the AU.S version of the SETROPTS and RACFCLAS reports are discussed in Chapter 8, "Auditing system integrity and security," on page 67.For more detailed information, see Figure 55 on page 68 and Figure 57 on page 69.

To run SETROPTS reports and view class settings, complete the following steps:

1. Select option **RA** (RACF Administration).
2. Select option **S** (Settings) to open the SETROPTS and class settings panel shown in Figure 34.

```
zSecure Admin+Audit for RACF Display Selection         1 s elapsed, 0.6 s CPU
Command ===>_____________________________________________ Scroll===> CSR_

  Name     Summary Records Title
_ SETROPTS       1       1 RACF SETROPTS system settings
_ RACFCLAS     208     208 RACF class settings
_ RRSFNODE       0       0 RACF remote sharing facility nodes
****************************** Bottom of Data ********************************
```

Figure 34. SETROPTS and class settings panel

As you can see in Figure 34, the SETROPTS and RACFCLAS reports are automatically generated.

3. In the **SETROPTS** selection field, type the **S** command to open the SETROPTS report shown in Figure 35 on page 38.

```
RACF SETROPTS system settings                                    Line 1 of 68
Command ===>_____________________________________________ Scroll===> CSR_
                                          15 Apr 2005 11:19

Complex  System
DEMO     DEMO

General RACF properties                Data set protection options
Access Control active          Yes     Prevent duplicate datasets    No
Force storage below 16M        No      Protectall                    Yes/fail
Check all connects  GRPLIST    Yes     Automatic Dataset Protect     No
Check genericowner for create  Yes     Enhanced Generic Naming       Yes
NOADDCREATOR is active         Yes     Prefix one-level dsns         ONEQUAL
Dynamic CDT active             No      Prevent uncataloged dsns      Yes/fail
RACF local node                DEMO    GDG modelling                 No
RRSF propagate RACF commands   No      USER modelling                No
RRSF propagate applications    No      GROUP modelling               No
RRSF propagate passwords       No
RRSF honour RACLINK PWSYNC     Yes
Application ID mapping stage   0
Level of KERB processing        0
Primary Language               ENU
Secondary Language             ENU
```

Figure 35. RACF settings SETROPTS report

You can use this report to investigate the RACF system-wide settings. You can use PF7 and PF8 for scrolling the report up and down.

Note: This report is available only in zSecure Admin.

Additionally, you can administer the majority of the SETROPTS options from this panel by typing over the current value with the desired value for the SETROPTS setting you want to change. This action automatically generates the appropriate SETROPTS command to apply the change.

Press PF3 to return to the SETROPTS and Class Settings Panel.

To view the class settings report, complete the following steps:

a. Enter the **S** command in the RACFCLAS report selection field to open the RACF class settings panel shown in Figure 36.

```
RACF class settings                                          Line 1 of 197
Command ===>_____________________________________________ Scroll===> CSR_
                                          15 Apr 2005 11:19
   Class    Active Description
_ ACCTNUM  Active TSO account numbers
_ ACICSPCT Active CICS program control table
_ AIMS     Active IMS application group names (AGN)
_ ALCSAUTH ______ Supports the Airline Control System/MVS (ALCS/MVS) product
_ APPCLU   Active Verify ID of partner logical units during VTAM session estab
_ APPCPORT Active Controls which user IDs can access the system from a given L
_ APPCSERV Active Controls whether a program being run by user can act as a se
_ APPCSI   ______ Controls access to APPC side information files
_ APPCTP   ______ Controls the use of APPC transaction programs
_ APPL     Active Controls access to applications
_ BCICSPCT Active Resource group class for ACICSPCT class
_ CACHECLS ______ Profiles for saving and restoring cache contents
_ CBIND    ______ Controls the client's ability to bind to the server
_ CCICSCMD Active Used to verify that user is permitted to use CICS syst prog
_ CIMS     ______ IMS command resource group
_ CONSOLE  Active Controls access to MCS consoles
_ CPSMOBJ  ______ Used by CICSPlex SysMgr for operational controls
```

Figure 36. RACF settings RACFCLAS report

b. To view the full detail settings of the involved resource class, enter the **S** line command in the **Class** selection field.

c. Optionally, you can enter the **R** line command to refresh the involved resource class or type over the existing value in the **Active** column. You can type: **Y**, **A**, or **Active** to activate a resource class that is currently inactive. Type **N** or blanks to deactivate a resource class that is currently active.

   Note: This functionality is available only in zSecure Admin.

Chapter 4. Using distributed and scoped administration functions

This section describes the distributed administration functions, which are only a selected subset of the administrative functions available. This section also provides information about the group auditor view.

Administering groups using RACF scope

Note
This function is available only in zSecure Admin.

To limit functionality to a group administrator's natural RACF scope, the program must be run in restricted mode. You can achieve this requirement by using any of the following methods:

Method 1
Create an `XFACILIT` profile `CKR.READALL` with UACC(NONE) and give only central administrators READ permits.

This method is the easiest and most suited for an evaluation.

Method 2
Access the RACF database through Program Access to Data Sets (PADS). This can be overridden by issuing a READ permit on the `XFACILIT` profile `CKR.READALL`.

This method is the safest but can be difficult to set up.

Method 3
Use a `SIMULATE RESTRICT` command in `SETUP PREAMBLE`.

This method works only to test your own scope.

Method 4

Issue the command `SETUP VIEW` and select **1** or **2** under **Select view**:

1. Enables you to view only profiles you are authorized to change (administrator view).
2. Enables you to view only profiles you are authorized to change or list.

This method provides an additional scope restriction. However, this scope restriction is not called restricted mode, but administrator view.

Like method 3, this method works only to test your own scope. It prevents you from displaying profiles that you have only READ access to, and it ignores system-wide privileges, so it is even more restrictive than the natural RACF scope.

Accessing the Quick Administration panel

Note
This function is available only in zSecure Admin.

You can access the Quick Admin function using one of the following two methods:

Method 1

- Select option **X** (Exit) from the Main menu.
- Type **CKR,STARTTRX(MENU(RA.Q))** in the command line under ISPF Option **6** to start the Quick Admin application. See Figure 37.

Method 2

Select **RA.Q** from the Main menu to open the Quick Admin panel shown in Figure 37.

You can use the Quick Admin panel to access the most frequently used functions required by a central or decentralized user administrators, hiding the details.

The Quick Admin panel relies on the system or group-SPECIAL attribute of the administrator. The options in the panel can be hidden by `CKR.OPTION.RA.Q...` profiles, but otherwise the menu works as shown.

```
   Menu   Options   Info   Commands   Setup     StartPanel
------------------------------------------------------------------------------
                zSecure Admin – RACF - Quick admin
 Command ===> ____________________________________________________________

1    Password        Set new password for user
2    Resume          Make sure user can work
3    Display         List user definition
4    Modify          Change user definition
5    Connect         Add group to a user
6    Add user        Create new userid from scratch
7    Add user copy   Create new userid like existing model
8    Phrase          Set new password phrase for user

Userid  . . . . . . ________     (type userid and press enter)
New password  . . .              (type new password, option 1 only)
Verify password . .              (type new password again, option 1 only)
Group   . . . . . . ________     (type connect group, option 5 only)
```

Figure 37. Quick Admin

Using CKG scope for group administration

Note

This function is available only in zSecure Admin.

zSecure Admin provides the CKGRACF program as the base for distributed RACF control; that is, Helpdesk and Group Admin. The CKGRACF program is designed to provide the following functionality:

- Access to commonly used Helpdesk functions such as password reset through menus.
- Access to commonly used Group Admin functions such as permits and connects through menus.
- Access to Helpdesk and admin functions *without* granting group-SPECIAL authority.
- Granular controls over user authorization to use CKGRACF functions.

CKGRACF differs from the main CKRCARLA program in that it performs most of its tasks through APF-authorized interfaces, whereas the main program generates normal RACF commands whenever possible. Because APF-authorization is required, the user of the main CKRCARLA program must have sufficient administrative RACF authority to execute the generated RACF commands. These commands are generated when you overtype a parameter, or use line commands to change profiles. The main zSecure Admin ISPF panels sometimes call the CKRCARLA program to make RACF changes when no standard RACF command can be generated to make the required change. Updating user data fields is the best example of this.

The CKGRACF user does not require any special RACF authority such as the SPECIAL or group-SPECIAL attribute. The CKGRACF program, using APF interfaces, adopts whatever authority it needs for a task. Therefore, you must control who can use the CKGRACF program by putting each CKGRACF user or group of users in the access control lists of several `XFACILIT` class profiles. By creating these profiles and PERMITing selected users, you can control who can perform specific functions through CKGRACF.

This section addresses two categories of CKGRACF users:

- Help desk users issuing commands such as password reset and resume.
- Decentralized administrators issuing permits or connects.

The Helpdesk functions are performed from a separate panel, while the group administrator's functions are available through the normal zSecure Admin panels. You can tailor the menus by adding RACF profiles in the XFACILIT class. Each profile represents a function. Access is granted using the usual access rules. By default all options are shown, but after you have implemented a tailored menu, only the granted functions are shown to the zSecure Admin user.

For your evaluation, give yourself full authority for all CKGRACF functions and then explore the functions. Setting up the XFACILIT class controls for a realistic group of distributed administrators should be a one-time job, but it can be tedious. It involves the following steps:

1. Defining exactly which RACF groups are associated with which administrators
2. Defining which CKGRACF functions are to be given to which administrators
3. Creating the necessary `RDEFINE` and `PERMIT` commands to create this environment

Because of the amount of time required to define the class controls, complete your initial product evaluation without attempting to establish granular controls.

To give yourself full CKGRACF authority, you or someone with RACF SPECIAL authority must issue the following RACF command:

```
permit ckg.** class(xfacilit) acc(update) id(yourid)
```

Accessing the single panel Helpdesk

Note
This function is available only in zSecure Admin.

You can access the Helpdesk function using one of the following methods:

Method 1

- Select option **X** (Exit) from the Main menu.
- Type **CKR,STARTTRX(MENU(RA.H))** in the command line under ISPF Option **6** to start the Helpdesk functions. See Figure 38.

Method 2

Select **RA.H** from the Main menu to open the Helpdesk panel shown in Figure 38.

Use this panel to perform the most frequently used functions required by a central or decentralized Helpdesk employee.

To see how the Helpdesk function works, complete the following steps:

1. Type a userid in the **Userid** field.
2. Press Enter to open the Helpdesk panel displaying the selected information about the userid as shown in Figure 38.

```
 Menu   Options   Info   Commands   Setup     StartPanel
------------------------------------------------------------------------------
                zSecure Admin – RACF - Helpdesk
Option  ===> ____________________________________________________________

1    List            List RACF profile information
2    Password        Set a new password
3    Default         Set the password to the user's default value
4    Previous        Set the password to the previous value
5    Resume          Resume a userid after too many password attempts
6    Disable         Temporarily disable logon for a userid
7    Enable          Allow user to logon after a Disable
8    Set default     Define a default password for a userid

Userid  . . . . . ________     (type userid and press enter)
New password  . . .            (type new password)
Verify password . .            (type new password again)
Reason  . . . . . ____________________________________________________
Workflow option . . 1      1. Request  2. Withdraw  3. Approve  4. Deny
```

Figure 38. Single panel Helpdesk

3. To see the user details, select **1** in the Helpdesk panel.

Now that you have checked the status of the userid, you can make changes, such as setting a new password (option **2**).

In the initial configuration, you see the `CKGRACF` command before it is executed. To suppress this confirmation prompt for individual administrators, type **setup confirm** in the command line or use the **Set default** option (option **8**) to suppress the prompt for all administrators.

Using the Helpdesk

> **Note**
> This function is available only in zSecure Admin.

Perhaps the most important CKGRACF functions for the Helpdesk are related to passwords, and revoke or resume. The following table lists the available functions and describes how they work.

Table 4. Helpdesk password-related functions

Helpdesk function	Description
Set a new password (option 2)	Set a new password, and enter it twice. zSecure Admin and zSecure Audit for RACF do not use RACF to update the user profile. `CKGRACF` authority is used instead. The user is also resumed.
Enable a default password (option 3)	The password is set to the default password for the user. A central administrator must have previously set the personal default password for the user. The Helpdesk administrator does not see the password. The user is also resumed.
Enable the previous password (option 4)	The previous password is enabled again. In this case, the administrator does not see the password. The previous password is automatically marked as expired; the user can use it only one more time for the next logon. The user is also resumed.
Set default (option 8)	Define a default password for a userid.

The concept of a default password (Option 3) is new to RACF. The intention is that a simple (and perhaps low-quality) password be defined for each user, with each user selecting a word or number that can be remembered indefinitely. Only the central RACF administrator sees this word when it is established using CKGRACF. Other administrators do not see it when it is called. If a normal password for the user becomes unavailable for some reason, any Helpdesk administrator can enable the default password for the user. The user is expected to create a new normal password as soon as possible. This approach is better than using system-wide reset passwords, such as SYS1, SECRET, PSWPSW, for example.

Tailoring the Helpdesk

You can tailor the Helpdesk panel for the installation in either of the following ways:

- Through `XFACILIT` profiles starting with `CKR.OPTION.RA.H`, you can selectively enable and disable options in the Helpdesk .
- Using `SETUP NLS`, you can modify the text and options in the panel.

Some functions, like setting the default password or a new password, or setting authority levels, are user management functions and should be available to a limited number of people. You can define `CKR.OPTION` profiles in the XFACILIT class to restrict the use of management functions. Thus, the installation can specify which options are shown in the Helpdesk panel for each user and selectively delegate responsibilities in the organization.

If the access control list of the corresponding profile grants a user access, the user is allowed to perform the function. Otherwise the line command is not shown in the action list and its use is prohibited. Figure 39 on page 46 shows an example of a tailored Helpdesk panel that does not contain the options 2, 6 and 8 because the user lacks the required access in the applicable `CKR.OPTION.RA.H` profiles.

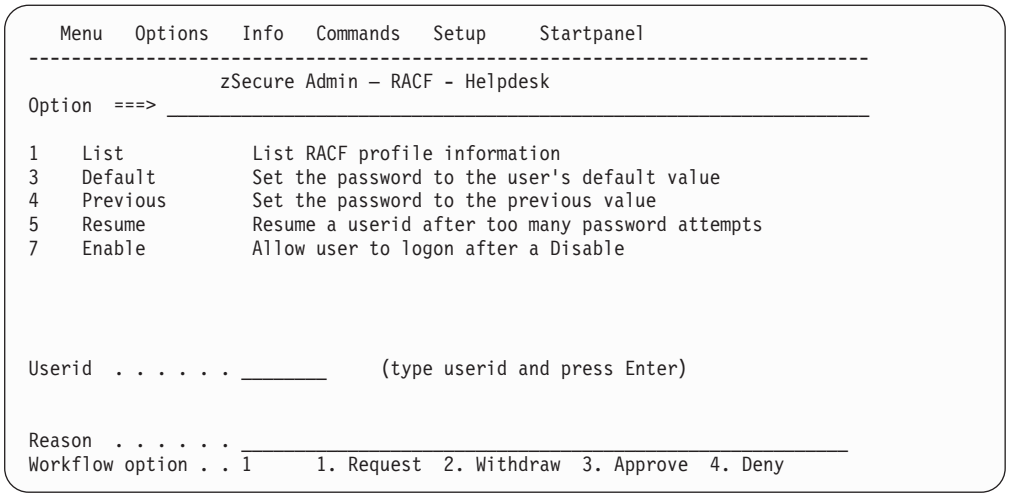

Figure 39. Tailored Helpdesk panel

Chapter 5. Managing data with the Setup functions

The Setup functions control which data is used by zSecure Admin and zSecure Audit for RACF, and enable you to switch data sources while using them. Other Setup functions set global switches and parameters. You have already seen some of these with the Resolve and Explode options.

Adding data

So far, you have used only your live RACF data to display various profiles. This section teaches you how to create and use the following additional data sources:

- An unloaded RACF database.
- A CKFREEZE data set that contains extracted information from all your DASD and from various internal z/OS tables.

To begin this process, complete the following steps:

1. Return to the Main menu, using PF3, as necessary.
2. Select option **SE (Setup)** to open the Setup panel shown in Figure 40.
3. If you are on a 24-line display, press PF8 and PF7 to scroll up and down in the panel.

   Tip: Before continuing, you can select Options **0** through **5** (one at a time) in the Setup panel to obtain a general overview of the various setup options.

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                  zSecure Admin+Audit for RACF - Setup
Command ===> ____________________________________________________________

0    Run             Specify run options
1    Input files     Select and maintain sets of input data sets
2    New files       Allocate new data sets for UNLOAD and CKFREEZE
3    Preamble        Carla commands run before every query
4    Confirm         Specify command generation options
5    View            Specify view options
6    Instdata        Customize installation data appearance
7    Output          Specify output options
8    Command files   Select and maintain command library
U    User defined    User defined input sources
C    Change Track    Maintain Change Tracking parameters
N    NLS             National language support
T    Trace           Set trace flags and CARLa listing for diagnostic purposes
D    Default         Set system defaults
R    Reset           Reset to system defaults
I    Installation    Specify installation defined names
```

Figure 40. Setup

Adding new files

To input new files, complete the following steps:

1. From the initial Setup panel, shown in Figure 40, select Option **2 (New files)** to open the New files panel shown in Figure 41 on page 48.

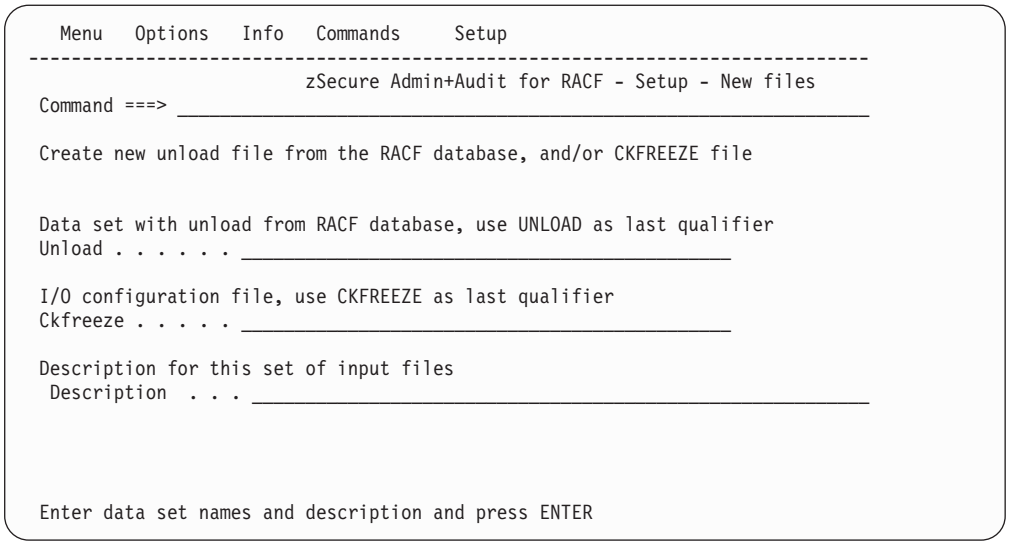

Figure 41. New files panel

2. Type a data set name in the **Unload** line.

   An input set can contain multiple coherent files.

   When entering the data set names, use quotation marks if necessary; that is, if the dataset names should not have your userid as the high-level qualifier. It does not matter whether these data sets exist yet. However, if they do exist, they must be cataloged.
3. Type a data set name in the CKFREEZE line, using quotation marks if necessary.
4. Type a short, unique description of the files in the **Description** line. For example, `UNLOAD and CKFREEZE data sets created on 8 Apr 2005`.

   Tip: It is a good practice to use the input file **Description** field to indicate what kind of data sets are part of this set. In the future, this can prevent the need to open the set in browse or edit mode to examine which data sets are included.
5. Press Enter.

   If one or both of the data set names you have specified do not exist, the allocation entry panel shown in Figure 42 on page 49 opens to allocate and catalog the new data sets.

```
 Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                        zSecure Suite - Setup - New files
Command ===> ____________________________________________________________________

CKFREEZE file not found. Change dataset name, or specify allocation parameters

 Dataset name . . . MYNAME.CKFREEZE_____________________________

Allocation parameters to create new dataset:
 Volume serial  . . ______      (Blank for authorized default volume)
 Generic unit   . . ________    (Generic group name)
 Space units  . . . _____       (KB, TRKS, or CYLS)
 Primary quantity   ________    (In above units, press HELP for suggestion)
 Secondary quantity ________    (In above units)

 Record format  . . VBS__       (VB or VBS)
 Block size   . . . 27998__
 Logical Record Len X______     (X or maximum record length)

Press ENTER to allocate dataset, press END to stop processing
```

Figure 42. Typical allocation panel

6. Type the appropriate allocation parameters, but do not change the DCB attributes.
7. Press Enter.

   You see the allocation panel a second time if both named data sets are new. Running these panels allocates and catalogs your new data sets using dynamic allocation. The first time you create an unloaded RACF copy and a CKFREEZE data set, you must specify ample disk space. For RACF unloads, allow as much space as used by your live RACF database. For CKFREEZE files, allow at least 2 MB for each online volume, plus space for catalog and HSM information.

   Do not alter the DCB parameters. Until you are familiar with the disk space required, specify a large secondary allocation quantity (such as 100 MB).

   Tip: After creating your first unloaded RACF copy and CKFREEZE data sets, use ISPF to examine them to determine how much disk space was actually used. This information makes estimating future usage easier.

   After the files have been allocated, the panel shown in Figure 43 opens.

```
  Menu   Options   Info   Commands     Setup
--------------------------------------------------------------------------------
                        zSecure Audit for RACF - Setup - Input fi Row 2 from 3
Command ===> ____________________________________________ Scroll ===> CSR_
Enter REFRESH on command line and press ENTER to generate UNLOAD job
Description . . . . Unload_and_CKFREEZE_data_sets_created_8_Apr_2005___________
Complex . . . . . ________   Version  . . . .  ____
RRSF node . . . . ________   Local node for RRSF

Enter data set names and types.         Type END or press PF3 when complete.
Enter dsname with .* to get a list      Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D            Type REFRESH to submit unload  job.

   Data set name or DNSPREF=, or Unix file name           Type        NJE node
_  'HLQ.CKR.SDEMO.UNLOAD'                                 UNLOAD      ________
_  'HLQ.CKR.SDEMO.CKFREEZE'                               CKFREEZE    ________
****************************** Bottom of data ********************************
```

Figure 43. Input file panel to define data set definition

Refreshing and loading files

The data sets listed constitute one input set. An input set can contain multiple CKFREEZE data sets, multiple SMF files, and multiple HTTP log files. However, an input set can contain only one RACF unload, or one or more RACF data sets (from one split database).

To refresh and load files, complete the following steps:

1. In the Input file panel (Figure 43 on page 49), type **REFRESH** in the command line. Then press Enter to open the Job submission panel.
2. In the Job submission panel, type a valid job card in the **Job statement information** section.
3. Use the **Edit JCL Option (2)** to open the normal ISPF editor to customize the JOB statement and make any other necessary changes to the job.

   For example, you might need a `JOBLIB` or `STEPLIB` statement to access zSecure Admin and zSecure Audit for RACF. If you copied zSecure Collect for z/OS (CKFCOLL) to an authorized library in the LNKLST, you do not need a `JOBLIB` or `STEPLIB` statement for it. Assign a job class with a large or unlimited region size.
4. Submit the job.

Wait until the job runs. If there is a long queue of jobs waiting to run, you can exit from zSecure Admin and zSecure Audit for RACF while the job completes. The job itself takes only a few minutes to run, unless you have a very large configuration. You can add a `NOTIFY=`*`yourid`* in the job card. If the job fails, the problem is usually that there is not enough storage. A region size of 64 MB is usually sufficient to run zSecure Collect for z/OS.

After the job is completed, continue with the next procedure.

Selecting the input set

To select the input set, complete the following steps:

1. To open the Input file panel, type **SE.1** (Option **1** on the Setup panel) in the **Command** line.

   The Input file panel should look like the input set you just created, with the description you entered for the input files. An example is shown in Figure 44.

```
 Menu   Options   Info   Commands     Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setup - I Row 1 from 4
Command ===> ____________________________________________ Scroll ===> CSR_

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

   Description                                              Complex
_  UNLOAD and CKFREEZE data sets created 8 Apr 2005                 selected
_  Active backup RACF data base                             DEMO     selected
_  Active primary RACF data base                            DEMO
_  Active backup RACF data base and live SMF data sets      DEMO     selected
****************************** Bottom of data ********************************
```

Figure 44. Input file selection

In Figure 44, the input file sets marked as `selected` indicate that zSecure Admin and zSecure Audit for RACF are now using these input sets for the input data. The other input sets (Active primary RACF data base, Active

backup RACF data base, Active backup RACF data base and live SMF data sets) are always present. You can switch to any input set defined in this display. For example, you can switch between the unloaded files you just created and the live RACF databases by going to this panel and selecting the appropriate input set.

To select an input set, type **S** in the entry field for that input set. You can change input selections many times during a session, although this is not typical usage.

2. Type **U** to remove the selection from **Active backup RACF data base and live SMF data sets** that is currently selected.

Using other Setup parameters

The Setup panel sets a number of allocation and formatting characteristics for zSecure Admin and zSecure Audit for RACF. Inspect these settings and make any necessary changes; the default settings are appropriate for most users. The most used Setup options are the Confirm and View options.

Setting up INSTDATA

Use the INSTDATA parameter to define the layout of the installation data field so that it can be displayed in business-oriented terms in the standard panels.

Setting up View

Information about the View options is available in "Changing the access list display settings" on page 23. The following sections describe the remaining settings of the View options and the Confirm options.

The **ACL/Connect sort** selection defines the access control list and connects sort order. It performs the following types of sorts:

- By ID (user or group in the access control list) if you select option **1**.
- By Userid (after exploding) if you select option **2**.
- By descending access level (Alter-None) or connect authority (Join-Use) if you select option **3**.

These sort options make scanning the ACL and connect easy and help you to find what you are looking for quickly.

You can use the **Show OS specific options** selection to switch between z/OS and z/VM® specific options, or tag both to see all options.

When you select the **Add summary to RA displays for multiple complexes** option, an extra summary section is added to the display panels for options RA.U, RA.G, RA.D, and RA.R. The summary information shows profile differences when multiple complexes are selected. This setting is not saved in your ISPF profile. This option is enabled by default.

Use the **Add connect date and owner to RA.U connect group section** option to add the connect date and connect owner to the RA.U connect group section.

The **Add user/group info to view** parameter specifies whether to display information about users and groups (including connect groups) on ACLs. Although this setting provides more complete information, it causes zSecure Admin and zSecure Audit for RACF to use much more virtual storage, which requires a larger TSO region.

In the selection field for a parameter, type a **/** to set a switch on, or blank to set the switch off.

Setting up Output

The Output panel (Option **7** on the Setup panel) contains the **SMTP options**. You must specify these options if you want to e-mail reports through the **Send as e-mail** panel options or the **M (E-mail report)** action command in the Results panel. Ask your system programmer for the correct settings.

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                 zSecure Admin+Audit for RACF - Setup
Command ===> ____________________________________________________________

Report options for following runs
Pagelength . . . . _____
Linelength . . . . _____

_  Convert all printed output to uppercase

Print options                       SMTP options
Destination . . .  ________________  SMTP node . . . .  ________
Sysout class  . .  _                 SMTP sysout . . .  _
Writer id . . . .  ________          SMTP writer . . .  ________
Copies  . . . . .  ___
Character set . .  ____
FCB . . . . . . .  ____
Forms . . . . . .  ____
Output descriptor  ________
Forms overlay . .  __
```

Figure 45. Setup output definition panel

In the Setup Output panel shown in Figure 45, the **SMTP node** field specifies the job entry subsystem (JES) destination to which e-mails are routed for final processing. If the SMTP server is running on your local system, this field can be left blank or you can specify `local`.

The **SMTP sysout** field specifies the JES output class to be used for the SMTP output processing of e-mails.

The **SMTP writer** field specifies a name for use in SMTP selecting an e-mail `SYSOUT` data set. The external writer name is equal to the SMTP address space name. Usually this is SMTP.

Defining these SMTP options is required when using email as the output source.

Setting up Confirm

The Confirm panel (Option **4** of the Setup panel) is important.

Note: See “Generating and confirming RACF commands” on page 29 for additional information about the Confirm panel.

The first two parameters apply to zSecure Admin and refer to line commands (such as **D** (for delete) or **C** (for copy or clone) and field Overtype when displaying various profiles. These line commands generate RACF commands. You can control the steps and execution of commands by selecting your desired values in the Confirm panel. Type a **/** before a profile, and then press Enter to see the available commands.

Table 5 shows the **Action on command** option settings and descriptions.

Table 5. Action on command option settings and descriptions

Action on command	Description
1. Queue	RACF change commands (automatically generated when you use a line command) are written to the `CKRCMD` file.
2. Execute	The automatically generated RACF commands are immediately executed, after confirmation, in RACF.
3. Not allowed	No update line commands (like **C** and **D**) are permitted in the profile detail panel. Any line commands that are issued are denied.
Execute display commands (for option 1 only)	This option is valid only if you specify option **1** (Queue) for the **Action on command** field. If you specify this option, list commands like LISTUSER, PING, TRACERTE, and RLIST are executed even though **Action on command** is set to **Queue**. This option applies only to the commands generated by the program as list commands. If you change or add commands yourself, it does not apply. For example, FORALL treats all sorts of commands as ordinary commands even if you typed in `LISTUSER`.

The **confirmation** setting indicates the disposition of the RACF commands generated by zSecure Admin. Table 6 shows the **confirmation** option settings and descriptions.

Table 6. Confirmation settings and descriptions

Confirmation	Description
1. None	No RACF change commands must be confirmed. **None** disables the verification prompt; use it only when you understand how to use zSecure Admin.
2. Deletes	Only Delete commands must be confirmed.
3. Passwords	Commands containing a *readable* RACF password are not confirmed. All other commands must be confirmed.
4. All	The user must confirm all change commands.

Tip: Regardless of the preceding settings, you cannot use the facilities described here to alter the RACF database without having the required authority, such as group-SPECIAL, to change the RACF profiles.

The **Command routing** option determines how generated commands are processed. Table 7 describes the available command routing options.

Table 7. Command routing settings and descriptions

Confirmation	Description
1. Ask	**Ask** is the maximum prompting level. For all commands or command files, the user is prompted for command routing information. This setting applies to commands generated for the local system, as well as for commands generated from data sources that are known to be from other systems.

Table 7. Command routing settings and descriptions (continued)

Confirmation	Description
2. Normal	**Normal** is the default prompting level for command routing. Both internally generated commands and bulk commands that are always queued are run without prompting for command routing options. Confirmation prompting and command queuing are done based on the settings for the user. If the RACF data source applies to the local system, commands are routed to the local system. The user can specify any of the following remote options for a local data source `RRSFNODE`, `ZSECNODE` or `JESNODE`. These remote indicators are ignored for a local data source. If the commands are not for the local system, they are routed to one of the following systems in order of preference: 1. The `ZSECNODE` or the `ZSECSYS` as specified on the RACF data source used for this profile. 2. The `RRSFNODE` node associated with the RACF data source used for this profile. The command uses the AT keyword, specifying either the associated userid if the terminal user has an association with a userid on the target `RRSFNODE`, or the current userid. 3. The NJE node specified for the RACF data source If a specific routing mechanism is selected and fails, there is no automatic fallback to another routing mechanism.
3. Local only	Independent of the input source, this option routes the command to the local system. If the local system is part of an RRSF autocommand environment, RRSF processing might route this command to other RRSF nodes.

The **Overtype fields in panels** option in the Command generation section of the panel enables you to modify many fields while displaying profiles, if you are running zSecure Admin. Based on the modifications, zSecure Admin and zSecure Audit for RACF automatically generate the RACF commands necessary to make the desired changes. These change commands are also subject to the action on command and confirmation settings described above. The ability to modify fields is one of the most important usability features, as it provides a very easy way to make minor changes in existing RACF profiles.

All zSecure Admin and zSecure Audit for RACF setup parameters are saved in your personal ISPF profile data set. Therefore, each user can have different setup parameters. If you access zSecure Admin and zSecure Audit for RACF using multiple userids, you might have different setup parameters for each userid.

Change values and verifying

This example uses the **RA.U** function that you are already familiar with to illustrate the ability to change values using the Overtype function and verify options.

To demonstrate these options, complete the following steps:

1. Go to the Main menu. (Press PF3 as necessary.)
2. From the Main menu, select option **RA** (RACF Administration).
3. Select option **U** (User).

4. Type a value for **Userid** or type a value for **Default group** (SYS1, for example) to obtain a display with multiple profiles.

   You can type over a value in any underlined field. For example, to change the password interval for one of the profiles, type a new value in the **PwInt** column.

   Tip: If no fields are underlined, type **SET** in the command line and press Enter. Verify that the **Overtype fields in panels** option is selected (**/** in front of the option).

   If this does not work, complete the following steps:

   a. Type **SETUP** in the **Command** field to go to the Setup panel.
   b. In the Setup panel, select **Options** from the bar. Press Enter, and then select **1. Settings**.
   c. Select **Colors** from the bar, and then select **2. CUA attributes**.
   d. For all entry field rows change the Highlight column to the value USCORE.
   e. Reissue the query.

      If you still do not see underlines, you probably have, or emulate, a terminal type without extended data stream support.

5. Press Enter.

   zSecure Admin generates the appropriate RACF command to change the password interval of the involved user and asks you to verify the command before execution.

   Remember to scroll left and right using the standard ISPF function keys, and to issue an **S** (Select) line command for more details.

6. Press PF3 to reject (not execute) the RACF command, *or* press Enter to submit the RACF command.

   If you elected to submit the command, zSecure Admin for RACF submits the command as though you had entered the command in the TSO command line. You must have appropriate authority (for example, SPECIAL or ownership) before RACF accepts the command. If you do not have appropriate authority, you receive a RACF violation error message.

   You can type over the value in the installation data field in a profile, changing only the characters you want to change. Alternatively, you can issue the **MI** (manage userid information) line command to edit the whole field. You can also work with user-defined subfields within the installation data.

Using line commands and the Overtype functions

When displaying a profile, you can issue line commands by typing a letter in the first character position of the displayed profile line and pressing Enter.

The most common functions are as follows:

C for copy

D for delete

L for list

S for select

When you issue a line command, zSecure Admin and zSecure Audit for RACF generate the appropriate RACF commands to perform the requested function. A

common technique is to use the **Copy** line command to reproduce a profile, and then type over the values in the fields that you want to be different in the new profile later.

The **L** line command executes a RACF list command in the primary RACF database for the profile you issue the **L** for. You can also use this command in a detail display.

Note: The **L** line command always reports from the primary RACF database.

To view a list of the line commands available in a profile overview display, type the **/** line command. For the RA.U function, you must scroll down (PF8) to see all of the application line commands.

Chapter 6. Reporting

All reports, and several other functions, generate the Results panel.

From the IBM Security zSecure Admin and Audit for RACF Main menu, complete the following steps:

1. Select option **RA** (RACF Administration).
2. Select option **3** (Reports).

   On the next panel, you can select one of the predefined reports.
3. Select option **4** (Permit/Scope).

On the Report panel, create a report that shows you the scope of the specified user:

1. Type a userid. (For this exercise, it does not matter whose userid you enter.)
2. Specify **3** (type of authorization is Scope – Access or administrative authority by any means).
3. Type a **/** in front of **Output in print format** in the **Specify output options** section of the screen and press Enter.
4. Press Enter in the next panel.

   On this panel, you can exclude some of the ways that the entered Group or User can have access to certain resources. During this evaluation, however, do not exclude any of the options so that you can explore all the methods by which a Group or User can have access to a resource.

zSecure Admin and Audit for RACF searches the input RACF data. The report results are displayed on an overview panel that lists the classes and scope of access for the specified userid. To view detailed information about any class, type a **/** in the input entry field and press Enter. The panel shown in Figure 46 is displayed, with more detailed information about the selected class.

```
 BROWSE - IBMUSER.C2R10FE.REPORT     ———————————— LINE 0000 0.8 s CPU, RC=0
 COMMAND ===> _____________________________________________ SCROLL ===> PAGE
******************************** Top of Data ********************************
U S E R   A U T H O R I Z A T I O N   F O R   I D  IBMUSER  IBM DEFAULT USER

Class    Type    Profile name                                  Volume Access  Via
ACCTNUM  GENERIC **                                                  ALTER   IBM
APPCTP   GENERIC **                                                  READ    - U
CONSOLE          SDSF                                                ALTER   - W
DATASET  GLOBAL  &RACUID*.**                                         ALTER   - U
DATASET  GENERIC ANF.*.**                                            READ    - U
DATASET  GENERIC ANF.SANFLOAD                                        READ    - U
DATASET  GENERIC AOP.*.**                                            READ    - U
DATASET  GENERIC API.*.**                                            READ    - U
DATASET  GENERIC ASM.*.**                                            READ    - U
DATASET  GENERIC ASM.SASMMOD1                                        READ    - U
DATASET  GENERIC ASM.SASMMOD2                                        READ    - U
DATASET  GENERIC ASM.SASMSAM1                                        READ    - U
DATASET  GENERIC ASMA.*.**                                           READ    - U
DATASET  GENERIC ASMA.V1R2M0.SASMMOD1                                READ    - U
DATASET  GENERIC ASMA.V1R3M0.SASMMOD1                                READ    - U
DATASET  GENERIC ASMA.V1R3M0.SASMSAM1                                READ    - U
DATASET  GENERIC ASMT.*.**                                           READ    - U
DATASET  GENERIC ASMT.V1R2M0.SASMMOD2                                READ    - U
```

Figure 46. SCOPE report

After examining the report, press PF3 to produce the Results panel. See Figure 47.

Tip: If you want to produce a scope report that shows only the access a user has through his or her userid and group connects, select option **2** - Direct permit or Connect (Id or Connect Group on access list).

Using the Results panel

This panel is presented after many queries or functions; familiarize yourself with its operation. You can use the panel to review results in several different ways and save useful material from the functions. Useful material can include RACF commands generated by zSecure Admin and zSecure Audit for RACF while processing the last functions.

Reports overwrite the same files every time. That is, the files `SYSPRINT`, `REPORT`, `CKRCMD`, and so on, are rewritten every time the primary modules are called, so save any important results (using the **W** line command provided by the Results panel) before invoking another query or function.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
               zSecure Admin+Audit for RACF - Results
Command ===> ____________________________________________________________

The following selections are supported:
 B Browse file               S Default action (for each file)
 E Edit file                 R Run commands
 P Print file                J Submit Job to execute commands
 V View file                 M E-mail report
 W Write file into seq. or partitioned data set

Enter a selection in front of a highlighted line below:
_  SYSPRINT  messages
_  REPORT    printable reports
_  CKRTSPRT  output from the last TSO command(s)
_  CKRCMD    queued TSO commands
_  CKR2PASS  queued commands for IBM Security zSecure Admin
_  COMMANDS  zSecure Admin input commands from last query
_  SPFLIST   printable output from PRT primary command
_  OPTIONS   set print options
```

Figure 47. Results panel

The names of some of the files listed on the display are highlighted to indicate that the last operation generated data in these files. When applicable, you can browse, edit, save, run, or submit any of these files by using one of commands described in the top part of the Results panel, as appropriate.

Tip: You can use the **RESULTS** primary command in the command line of most panels to obtain the current Results panel.

To print DISPLAY results, use the **PRT** command.

Archiving report output

When you enter a **W** in front of the REPORT keyword in the Results panel, a panel opens where you can specify the data set name of an archive data set. The archive data set can be a sequential or a partitioned data set. For a sequential data set, you can write over the content by selecting **disposition Overwrite**, or append to the end of the current content by selecting **disposition Append**. For a partitioned data

set, you can specify a member name and the dispositions **Overwrite** or **Append**, or choose disposition of **Generate** and leave the member name blank. **Generate** assigns a unique member name to each report, so you do not need to choose a member name.

```
   Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
         zSecure Admin+Audit for RACF - Results of last query
Command ===> ____________________________________________________________

Write the zSecure Admin+Audit for RACF report file to the following dataset:
Data set name . . . . . ____________________________________________
Member  . . . . . ________
Disposition . . . . . _________  (Append, Overwrite, or Generate)

Processing option after Write completed:
Go into Edit  . . . . . N__        (Yes/No)
```

Figure 48. Archive output to a data set

If you specify a data set name that does not exist, zSecure Admin and zSecure Audit for RACF prompts you for allocation parameters:

1. Type the correct parameters and press Enter to create a new data set.
2. Press PF3 to exit from the Results panel.

   The Results panel exists after any search. However, it is automatically displayed only if files other than SYSPRINT contain output.

Tip: The next function you run overwrites these result data sets. If you want to save any of the data sets, do it before executing the next search.

Mailing report output

When you enter an **M** in front of the **REPORT** keyword in the Results panel, the email panel shown in Figure 49 opens so that you can specify to whom you want the report mailed.

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                                    zSecure Admin+Audit for RACF - E-mail
Command ===> ____________________________________________________________

Specify e-mail data
From  . . . . &jobname at &system <mbox@domain>_____________________________
Mail to . . . ____________________________________________________________
CC  . . . . . ____________________________________________________________
BCC . . . . . ____________________________________________________________
Reply to  . . ____________________________________________________________
Output format 1  1. Normal (MIME/HTML)
                 2. Plain text (formatting may be lost)
Font size . . _
Subject . . . ____________________________________________________________

Additional data (e.g. signature)
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
```

Figure 49. Email specification panel

The Mail option is valid only if you have specified SMTP configuration options in Setup Output definition panel (**SE.7**), as described in "Setting up Output" on page 52.

Chapter 7. Using the Verify functions

The Verify functionality helps you to analyze RACF and z/OS integrity and security data. For example, many of the functions compare RACF data with what actually exists on your disks (as seen by zSecure Collect for z/OS). In addition, most functions automatically generate RACF commands to correct problems found during the analysis phase. These commands are not automatically executed. They are merely presented for your review or use.

The first time you use Verify functions, you might receive more output than you expect, especially if you have a large installation that has been somewhat relaxed in DASD and RACF cleanup policies. There is a default limit of 50 messages per disk volume, but optionally you can override this limit through a lower-level panel. Product messages generated are concise and exact, but might take a little study to absorb. Also, *do not assume* that your installation must correct *all* the anomalies reported by all of the various Verify functions. Your installation, for example, might not agree with the security policies implicit in some reports. Use the information as appropriate, **but do not accept it blindly**.

After a Verify function completes, the results are presented (using the Results panel). Generally if RACF commands were generated, these commands are displayed first. Sometimes, the `SYSPRINT` output is presented directly after the completion of the Verify function.

The `SYSPRINT` file contains additional information about the problems found during analysis done by a Verify function such as concise descriptions of the anomalies and problems found during the analysis done by a Verify function. When you enter the command **find 'v e r i f y'** (a space between the characters is required, as are the delimiting single quotation marks) in the command line, you go directly to the M E S S A G E S V E R I F Y section of the `SYSPRINT` file.

To use the Verify function, complete the steps that follow:

1. Select option **AU** (Audit) from the Main menu.
2. Select option **V** (Verify) to open the Verify selection panel shown in Figure 50 on page 62.

```
   Menu  Options  Info  Commands  Setup          StartPanel
------------------------------------------------------------------------------
        zSecure Admin+Audit for RACF - Audit - Verify
Command ===> ____________________________________________________________

Enter "/" to select one or more options
_  Permit            Find undefined users and groups and their profiles
_  User permit       Find and remove redundant permits to userids
_  Connect           Compare USER, GROUP and CONNECT profiles
_  PADS              Programs on conditional access list have PROGRAM profile
_  Group tree        Loops in grouptree
_  Password          Userids with trivial passwords (not from an unloaded db)
_  Protect all       All datasets are protected by a (discr or gen) profile
_  On volume         Datasets defined by discrete profiles actually exist
_  Not empty         Generic profile has matching disk or tape datasets
_  All not empty     As above, even 'outer' generic profiles
_  Indicated         Discrete profile exists for RACF-indicated datasets
_  Program           Datasets as members in PROGRAM profile exist on disk
_  Pgm exists        PROGRAM profiles cover actual load modules
_  Started task      Check that procedures can indeed be started, etc.
_  TSO all RACF      All TSO users should have RACF password and TSO segment
_  Sensitive         Sensitive datasets not protected properly
```

Figure 50. Verify selection panel

You can select one or more of the Verify functions for execution, although it would be unusual to select more than three at a time. Before trying any of the Verify functions, review the function descriptions in Table 8 and Table 9 on page 63.

Table 8. Verify functions

Function	Description
Permit	Reports on any IDs (Users or Groups) used in RACF access control lists, or ownership fields, that are not currently defined as valid IDs. If these invalid IDs are defined again (made valid again), perhaps with a new user, this new user instantly inherits all the authorities of the former owner of that user ID. This can be a severe exposure. A more severe exposure is that anyone with group-SPECIAL or JOIN authority can create a group with the same name as the ID in the access control list, and in this way obtain the authority of the ID.
User Permit	Reports on any resource profile that contains a userid in the access control list, while that user is also connected to one or more groups that are also in the same access control list. The access levels of both the userid and the group or groups are compared. If the access for that specific userid is equal to the highest access of any connected group, the userid entry is redundant and is eligible for removal.
Connect	Verifies that connect information in user and group profiles is consistent.
PADS	PADS administration is often complicated, and several Verify functions address it. This function verifies that every program appearing on a RACF conditional access control list has a corresponding `Program` profile.
Group tree	Detects loops in your group definitions. These loops usually happen where RACF administration is not well centralized, or where administrators change frequently. RACF prevents loops from occurring by checking whether an `ALU` or `ALG` command would cause a loop.
Password	Checks every user password in the RACF database with several trivial values. The Password function cannot be performed on an Unload file, because the passwords are not unloaded.

The Verify functions described in Table 9 require a CKFREEZE data set.

Table 9. Verify functions requiring a CKFREEZE data set

Function	Description
Protect all	Lists all disk data sets that are not protected by a generic or discrete RACF profile. If your installation is using a RACF PROTECT ALL environment, try this function. If you are not in a PROTECT ALL environment, be prepared for a large amount of output.
On Volume	Verifies that each discrete RACF profile has a corresponding data set on DASD. Often old discrete profiles remain in RACF long after the data set has been deleted.
Not empty	Identifies obsolete generic profiles. This function verifies that generic dataset profiles that protect subsets of more general generic profiles have, in fact, existing data sets being protected by the generic profile. (Take care when using this function because profiles meant to protect future or periodic allocations might be *empty* (no data sets exist under the profile) at the time the Verify check is made.)
All not empty	This function is a more general case of the **Not empty** check. It verifies that all generic profiles are being used to protect real data sets. It can be used to find unneeded generic profiles. RACF and z/OS have no mechanism for automatically removing generic profiles, and large numbers of obsolete profiles can accumulate over time.
Indicated	Verifies that all RACF-indicated data sets (with RACF indicator bit set in the DSCB or catalog) have a corresponding discrete profile.
Program	Verifies that each data set listed as a member in a Program profile does exist.
Pgm exists	Verifies that each Program profile covers at least one load module in a data set, as specified by the profile. If modules are moved from one library to another, there is no automatic update of RACF Program profiles and the modules are no longer protected. The **Program** and **Pgm exists** functions help you to maintain a clean PADS environment.
Started task	Checks the consistency of the started procedure table (ICHRIN03) with various RACF user, group, and STARTED class profile definitions and with procedure members defined for JES2 and MSTR. **TSO all RACF** and **Sensitive** are available only in zSecure Audit.
TSO all RACF	Checks the users defined in the SYS1.UADS data set with the user definitions in RACF and reports any UADS IDs that can logon bypassing the control of RACF.
Sensitive	Checks the protection of z/OS sensitive data sets against a baseline policy. If the protection is insufficient, it generates a RACF command to fix the situation: either by adding a correct profile or by fixing or improving the offending profile.

Some of the Verify functions are more important than others. The Permit and Protect All functions might be the most important, especially if you are not in a PROTECT ALL environment.

To use the Verify function for the first time, complete these steps:

1. Type / in the **INDICATED** line.
2. Proceed through the next panel by pressing Enter.
   The CKRCMD command file shown in Figure 51 on page 64 automatically opens.

```
 File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       IBMUSER.C2R10FE.CKRCMD                        Columns 00001 00072
Command ===> _____________________________________________ Scroll ===> CSR_
Press PF3, Enter R at the cursor location, press ENTER to run these commands
000001         /* CKRCMD file CKR1CMD complex YESTERDY NJE JES2TEST generated
000002          /* Commands generated by VERIFY INDICATED  */
000003         addsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1) unit(3390) noset from(
000004         deldsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1)
000005         addsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1) unit(3390) noset from(
000006         deldsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1)
****** *************************** Bottom of Data ****************************
```

Figure 51. Verify the indicated CKRCMD file

In this example, the installation contains two data sets that are RACF indicated while the corresponding discrete dataset profile is missing from the RACF database. If necessary, use the ISPF functions PF7, PF8, PF10, and PF11 to scroll the panel so that you can view all the data.

As you can see, the generated commands can be run to fix the inconsistencies found by the Verify Indicated function.

3. Press PF3 to open the Results panel.
4. Select the SYSPRINT file if you want to view the details of the Verify function.

   The additional information is provided in the section headed by MESSAGES VERIFY INDICATED shown in Figure 52.
5. Type **find 'v e r i f y'** command on the command line to jump to the messages section of the SYSPRINT file instead of scrolling down several panels. Alternatively, you can scroll to the bottom of the file and, if applicable, scroll back up one or two pages. Figure 52 shows an example of the MESSAGES VERIFY INDICATED section.

```
 File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       IBMUSER.C2R10FE.CKRCMD                        Columns 00001 00072
Command ===> _____________________________________________ Scroll ===> CSR_
Press PF3, Enter R at the cursor location, press ENTER to run these commands
000001         /* CKRCMD file CKR1CMD complex YESTERDY NJE JES2TEST generated
000002          /* Commands generated by VERIFY INDICATED  */
000003         addsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1) unit(3390) noset from(
000004         deldsd 'IBMUSER.DISCRETE.DSN1' vol(TSTUS1)
000005         addsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1) unit(3390) noset from(
000006         deldsd 'IBMUSER.DISCRETE.DSN2' vol(TSTUS1)
****** *************************** Bottom of Data ****************************
```

Figure 52. Verify the indicated CKRCMD file

Note: The SYSPRINT file contains additional information about VERIFY messages is stored in.

6. To return to the Verify Selection panel, press PF3 twice.
7. Type a **/** in the **Permit** line.
8. Remove the **/** from the **Indicated** line.

   Step through the next panels until zSecure Admin and zSecure Audit for RACF executes the function.

   Unless you maintain a very clean database, zSecure Admin and zSecure Audit for RACF probably finds invalid userids in the database. If there are many of these userids, you can print the report and study it offline. Invalid userids can present complex problems that are not suitable for on-the-fly repairs.

Tip: When RACF commands are generated by one of the Verify functions, the solution suggested by zSecure Admin and zSecure Audit for RACF might not be appropriate or might require adjustment to your environment. Always look at the commands closely. If necessary, look in the `SYSPRINT` file for additional information before executing them.

Chapter 8. Auditing system integrity and security

The current SETROPTS settings can be displayed using the AU.S function.

A range of z/OS integrity and security checks is available under the AU.S option in the primary menu. For example, you can view the current SETROPTS settings using this function.

To use the AU.S function, complete the following steps:

1. Select option **AU** (Audit) from the Main menu.
2. Select option **S** (Status) to open the Audit Status panel.

   You can use this panel to select one to five report categories. First, explore the **RACF control** (RACF-oriented tables) category.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Audit - Status
Command ===> ____________________________________________________________

Enter / to select report categories
_  MVS tables           MVS oriented tables (reads first part of CKFREEZE)
_  MVS extended         MVS oriented tables (reads whole CKFREEZE)
/  RACF control         RACF oriented tables
_  RACF user            User oriented RACF tables and reports
_  RACF resource        Resource oriented RACF tables and reports



Select options for reports:                                  Audit policy
/  Select specific reports from selected categories          /  zSecure
_   Include audit concern overview in overall prio order     _  C1
_   Only show reports that may contain audit concerns        _  C2
__  Minimum audit priority for audit concerns (1-99)        _  B1
_   Print format              _  Concise (short) report
    _  Background run
```

Figure 53. Audit Status

3. Select the category **RACF control** and type a **/** before **Select specific reports from selected categories**. Press Enter.

   Note: The Audit policy can be set. The C1, C2, and B1 policies are security standards described by the U.S. Department of Defense in a document known as the *Orange book*. The default policy is a standard that is a practical and achievable security level that is applicable to most companies. The policy defines what is classified as an exposure.
4. Select the report **SETROPTS** to generate a report of the current RACF system options of this installation and the report **RACFCLAS** to report in the class descriptor table and number of profiles.
5. Press Enter to generate the requested reports.

   The panel shown in Figure 54 on page 68 opens so that you can select and view the reports.

```
                zSecure Admin+Audit for RACF Display   1 s elapsed, 0.6 s CPU
Command ===> ____________________________________________________ Scroll===> CSR_

  Name     Summary Records Title
_ SETROPTS       1       1 RACF system, ICHSECOP, and general SETROPTS settings
_ SETROPAU       1       3 SETROPTS settings - audit concerns
_ RACFCLAS       1     168 RACF CDT, SETROPTS class info and number of profiles
****************************** BOTTOM OF DATA ******************************
```

Figure 54. Audit report overview

6. Select the **SETROPTS** report. Then press Enter to open the SETROPTS setting panel shown in Figure 55.

```
RACF system, ICHSECOP, and general SETROPTS settings             Line 1 of 58
Command ===> ____________________________________________________ Scroll===> CSR_
                                              8 Apr 2005 08:46
   Complex  System   Collect timestamp
   DEMO     DEMO      8 Apr 2005 00:50

Current SETROPTS settings can be displayed using the AU.S function.
 General RACF properties                Data set protection options
 Access Control active         Yes      Prevent duplicate datasets    No
 Force storage below 16M       No       Protectall                    Yes/fail
 Check all connects  GRPLIST   Yes      Automatic Dataset Protect     No
 Check genericowner for create Yes      Enhanced Generic Naming       Yes
 NOADDCREATOR is active        Yes      Prefix one-level dsns         ONEQUAL
 Dynamic CDT active            No       Prevent uncataloged dsns      No
 RACF local node               DEMO     GDG modelling                 No
 RRSF propagate RACF commands  No       USER modelling                No
 RRSF propagate applications   No       GROUP modelling               No
 RRSF propagate passwords      No
 RRSF honour RACLINK PWSYNC    Yes
 Application ID mapping stage  0
 Level of KERB processing
 Primary Language              ENU
 Secondary Language            ENU
 RACF software release level   HRF7703 HRF7703
 RACF DB template level        HRF7703
```

Figure 55. Audit status SETROPTS report

The current SETROPTS (=SET RACF options) are listed in this report. You can use PF8 to scroll down to see the other SETROPTS parameters that are currently active, such as system-wide audit settings and password rules.

7. Press PF3 to return to the report overview.
8. Select SETROPAU to open the report shown in Figure 56.

   This report lists the audit concerns related to the current SETROPTS settings. Audit concerns give an indication of possible security exposures in the current installation.

```
                SETROPTS settings - audit concerns               Line 1 of 3
Command ===> ____________________________________________________ Scroll===> CSR_
                                              8 Apr 2005 08:46
   Pri Complex  System   Count
    11 DEMO     DEMO         3
   Pri Parameter               Value    Audit concern
__  11 RVARYSTATUSPWSET         No       Password to deactivate RACF still at I
__  10 RVARYSWITCHPWSET         No       Password to switch RACF database still
```

Figure 56. SETROPTS audit concerns overview

zSecure Audit for RACF ranks the severity of problems found. These are in the field labeled **Pri**, and are numbers from 0 - 255. Be aware, however, that

understanding the reason for those rankings requires some knowledge of z/OS internals and some judgment of the context of the total system. Table 10 provides a rough categorization of the audit concern priorities.

Table 10. Audit concern priority categories

Priority	Type	Explanation and action required
40-255	Exposure	A very serious potential security exposure and concern for an auditor. Require an immediate action.
20-39	Concern	A serious security threat. Require an action, but it is less urgent.
11-19	Housekeeping	Minor problem or authority that must be audited, reviewed, and approved or denied. RACF housekeeping can remove many these concerns.
1-10	Watch	Read it, and resolve it as time permits.
0	OK	No audit concern.

By default the Audit concerns are sorted by descending priority. The details of the audit concerns can be displayed by entering an **S** or **/** in front of the concern you want to view. To view the Audit concerns, complete the following steps:

1. Press PF3 again to return to the report overview.
2. Select report **RACFCLAS** and press Enter to open the Audit Status RACFCLAS report shown in Figure 57.

   This report displays the contents of the RACF Class Descriptor Table. You find a record for all classes defined to RACF.

```
                                                                Line 1 of 168
RACF CDT, SETROPTS class info and number of profiles
Command ===> _____________________________________________ Scroll===> CSR_
                                          8 Apr 2005 08:45
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
   DEMO     DEMO         168     59       58     2383            43       22
   Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
__ 22 DEVICES  115                   Inactive                     4      Ye
__ 20 TEMPDSN  106                   Inactive                     8      Ye
__  7 DASDVOL    0 GDASDVOL          Inactive                     3  4 OPER Ye
__  7 VMPOSIX   63                   Inactive      Discrete      16  4      Ye
__  6 SERVER   546                   Inactive      Discrete       1  8      Ye
__  6 TERMINAL   2 GTERMINL          Inactive                    11  4      Ye
__  6 VMCMD     14                   Inactive                     1  4 OPER Ye
__  6 VMMDISK   18                   Inactive                     9  4 OPER Ye
__  5 AIMS       4                   Inactive                     1  4      Ye
__  5 APPCTP    89                   Inactive                     2  8      Ye
__  5 GIMS       4          TIMS     Inactive                     9  4      Ye
__  5 JESINPUT 108                   Inactive                     2  8      Ye
__  5 PERFGRP  125                   Inactive                     1  4      Ye
__  5 ROLE     551                   Inactive      Discrete      16  8      Ye
__  5 SECDATA    9          SCDMBR   Inactive                     2  4      Ye
__  5 SECLABEL 117                   Inactive                     6  8      Ye
__  5 SYSMVIEW 542                   Inactive                     8  4      Ye
__  5 TIMS       4 GIMS              Inactive                    35  4      Ye
```

Figure 57. Audit status RACFCLAS report

In this report, the classes are sorted by descending audit concern priority. However, you can sort this overview ordered by any column that you desire. Entering command **sort pos** results in this overview being reordered according to **posit** number, while the command **sort class** results in the classes being sorted alphabetically by class name.

Tip: Remember that the available help panels provide background information and explanations.

Chapter 9. Querying SMF data

Note
The SMF Query function is available only in the zSecure Audit product.

The SMF displays can work with the live SMF data sets, SMF log streams, or with sequential SMF data that has been produced by the IBM IFASMFDP or IFASMFDL programs. While you are getting familiar and experimenting with zSecure Audit for RACF, work with sequential SMF data rather than the live SMF files. Using static, sequential data provides more consistent results when you retry something with slightly different parameters.

You must consider what SMF data you use with zSecure Audit. The amount of SMF data collected by z/OS varies greatly among different installations. In some cases, you can place a week of data in a reasonable DASD allocation (30 MB, for example), while in other cases, that allocation might hold only an hour of SMF data collection. For simple experimentation with zSecure Audit for RACF, a set of SMF data in the 10-30 MB range is reasonable. If you must apply filtering to reduce the size of the data set, make sure that the record types shown in Table 11 are not filtered out.

Table 11. SMF Record types that should not be filtered out of the SMF data

Record type	Description
14	INPUT or RDBACK Data Set Activity
15	OUTPUT, UPDATE, INOUT or OUTIN Data Set Activity
17	Scratch Data Set Status
18	Rename Data Set Status
30	Common Address Space Work
60	VSAM Volume Data Set Updated
61	ICF Define Activity
62	VSAM Component or Cluster Opened
63	VSAM Catalog Entry Defined
64	VSAM Component or Cluster Status
65	ICF Delete Activity
66	ICF Alter Activity
67	VSAM Catalog Entry Delete
68	VSAM Catalog Entry Renamed
69	VSAM Data Space, Defined, Extended or Deleted
80	RACF Processing
81	RACF Initialization
83	RACF Processing Record for Auditing Data Sets
90	System Status
92	UNIX Hierarchical File System
102	DB2® Performance and Audit
109	Firewall

Table 11. SMF Record types that should not be filtered out of the SMF data (continued)

Record type	Description
118	TCP/IP Telnet and FTP
119	TCP UDP and IP
120	WebSphere® Application Server

You can also run the zSecure Audit for RACF SMF analysis on a full SMF file with all record types present. The zSecure Audit for RACF supports approximately 100 different SMF record types.

Defining input sets

When you opt to process SMF data, the data sets must be defined to zSecure Audit for RACF. You can use live or log stream SMF data, or obtain a reasonable amount of recent SMF data and copy it to a sequential data set. In both cases, you must change your input files settings.

You can also run zSecure Audit for RACF SMF analysis on a full SMF file (with all record types present). The product supports about 100 different SMF record types.

To use a data set with SMF data, complete the following steps:

1. Select option **SE** (Setup) from the Main menu and press Enter.
2. Select **1** (Input Files) and press Enter to open the Setup Input panel.

   For information about this panel, see "Selecting the input set" on page 50.
3. Move the cursor to the input field (left-most position) on a line.
4. Type the letter **I** and press Enter to insert a new input set.

   The Setup Input panel opens but without data.
5. Type a title such as `Filtered SMF data set` in the **Description** field below the Command line.
6. Move the cursor to the first **Data set or Unix file name** field. Type the name of the data set that contains SMF data. Then press Enter.

   If the data set name ends with `.SMF`, the file type (SMF) is automatically filled in. If it does not end with `.SMF`, a panel such as Figure 58 on page 73 opens so that you can assign a type to the file you are defining.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Setu Row 1 to 13 of 13
Command ===> _____________________________________________ Scroll ===> CSR_


 Select the type of data set or file

     Type             Description
_    ACCESS           RACF ACCESS monitor data set
_    ACT.BACK         The backup RACF database of your active system
_    ACT.PRIM         The primary RACF database of your active system
_    ACT.SMF          The live SMF data set(s)
_    ACT.SYSTEM       Live settings
_    CKFREEZE         A CKFREEZE data set
_    CKRCMD           A file for generated RACF commands
_    COPY.RACF        A copy of a single data set RACF database
_    COPY.SEC         A non-first component of a multiple data set RACF database
_    COPY.TEMP        The first component of a multiple data set RACF database
_    SMF              VSAM or dumped SMF
_    SMF.LOGSTR       SMF logstream
_    UNLOAD           An unloaded RACF database
_    WEBACCESS        IBM HTTP Server access log
_    WEBERROR         IBM HTTP Server error log
```

Figure 58. Assign file type

7. Select option **SMF** and press Enter to create a line that references the live SMF data.
8. Press PF3.

   You return to the Input file panel with the new input set selected.

   Tip: You can select multiple input sets at the same time. Consider defining a set for each file or couple of files. For example, define a live SMF set and a most recent unload of the RACF database and CKFREEZE data set, and select both sets as input.

   Your input file settings will look similar to those in Figure 59.

```
 Menu   Options   Info   Commands  StartPanel
--------------------------------------------------------------------------------
      zSecure Admin+Audit for RACF - Setup - Input file       Row 1 from 5
Command ===> _____________________________________________ Scroll ===> CSR_

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

   Description                                            Complex
_  Filtered SMF data set                                          selected
_  Input set created 8 Apr 2005                                   selected
_  Active primary RACF data base                          DEMO
_  Active backup RACF data base                           DEMO
_  Active backup RACF data base and live SMF data sets    DEMO
****************************** Bottom of data ********************************
```

Figure 59. Input file settings

To use live SMF data you do not need to specify a data set. Type **/** in the **Type** field, and then press Enter. The panel in Figure 58 opens so that you can select option **ACT.SMF**.

This is the most basic form of SMF input. In a more complex situation, you can combine live SMF plus the most recent *n* generations, if you use Generation Data Groups (GDGs) of archived SMF data by listing multiple lines within the input set.

SMF reports

To create reports, complete the following steps:

1. Select option **EV** (Events) in the Main menu and then press Enter.
2. Select option **2** (RACF Events) and then press Enter.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
            zSecure Audit for RACF - Events - RACF events
Option  ===> ____________________________________________________________

Enter "/" to select report(s)
_ All events       Overview of all following RACF events (except IPL)
_ Logging          RACF logging of all events except RACINIT
_ Not normal       RACF access not due to normal profile access
_ Warnings         RACF access due to profiles in warning modes
_ Violations       RACF access violations
_ Commands         RACF command auditing
_ CKGRACF          zSecure Admin CKGRACF commands
_ IPL RACF         RACF initialization
```

Figure 60. SMF RACF events display

3. Select **All events** in the RACF events panel, and then press Enter.

   The SMF selection panel shown Figure 61 is common to a number of SMF reports.

```
  Menu         Options       Info    Commands     Setup
_______________________________________________________________________________
                        zSecure Admin+Audit for RACF "DOWN    " is not active
Command ===> ____________________________________________________________

Select SMF records that fit all of the following criteria
Use EGN masks for selection criteria
Userid  . . . . . . IBMUSER
Jobname . . . . . . ________________________________________________________
Terminal  . . . . . ________________________________________________________

Dataset name  . . . ________________________________________________________

Profile class . . . ________________________________________________________
Profile key . . . . ________________________________________________________
Level . . . . . . __   __      (installation defined resource level)

                    From         Until             Intended access at least
Time                ____       : ____              6  1. Execute  2. Read
Date                __________ : __________           3. Update   4. Control
Weekday             ____       : ____                5. Alter    6. All access

Show all            _  Success   _  Warning   _  Violation
```

Figure 61. SMF selection criteria

Only SMF records that match your specified selection criteria are processed. Any fields in this panel that you do not use are not considered in the selection process. For this panel:

- The **Userid**, **Jobname**, **Terminal**, **Profile class**, **Profile key**, and **Data set name** fields each accept one or more search strings separated by blanks. Wild cards (%, *, and **) can be used. A single asterisk in the **Userid** field, with no other parameters, selects all SMF records that can be attributed to a RACF user.
- You can use the **Level** field to select by data set or resource level.

Use the first field to specify the operator to determine a level present in the profile. Use < and <= for selection less than or equal to the level, > or >= for high level, = for exact level, ¬= and <> for all but the specified level.

The second field is to specify a numeric value for the data set or resource level. This level is not set or updated by IBM utilities, but can be used by the installation.

- Your userid is not automatically prefixed to data set names.
- Times are specified in 24-hour *HHMM* format.
- Dates are specified as *YYYY-MM-DD*, *DDMMMYYYY* or *YYYY/DDD*; for example, 2005-03-01, 01MAR2005, or 2005/301. A range of dates is separated by a colon; for example, 10APR2005:14APR2005.
- Weekdays are spelled in English using the first three letters; for example, Mon for Monday.
- In the **Intended access at least** field, you can select only access events that required, at least, the authority you specify.

After the selection panel, an exclusion panel opens, similar to Figure 61 on page 74. Be aware that the selection and exclusion panels look very similar. If an SMF record passes the selection process, it can still be rejected by the exclusion parameters. You do not need to specify any exclusion parameters. As an example, select all accesses to data sets with the name `SYS*.**` with access level at least UPDATE, but exclude access to data set `SYS1.BRODCAST`.

After the selection and exclusion panels, there are panels to control the report generated. These panels can be used to limit the number of input records. Especially if your SMF file is huge, limit the number of output records, and format output for displaying or printing.

For this example, do not select any CKFREEZE data set to use with SMF reports. Make sure that there is no **/** before **Use CKFREEZE data** in the SMF process options panel. For RACF-only purposes this option is not needed and can increase the TSO region size required. You *do* need this option to format UNIX file system records (type 92).

The SMF search produces an overview report with one line for each SMF record being displayed and a statistical summary. You can enter an **S** line command for a detailed display of any of the records.

zSecure Audit for RACF processing of SMF records is fairly straightforward. Its power lies in good use of the selection and exclusion panels and the high-speed processing. Nevertheless, effective use of SMF processing requires planning on your part so that you have reasonable amounts of recent SMF data available that is easily accessible on-line, or through HSM facilities.

zSecure Audit for RACF supplements any SMF event record with information from the RACF data source, if such information is missing from the record. In this way, z/OS event records like type 14 and 15 can be attributed to a RACF userid, even if the Jobname in the SMF record does not match the appearance of the RACF userid.

Auditing types of users

To audit a user event trail, you must have an input data set that contains SMF data selected first. Then complete the following steps:

1. Return to the Main menu.

2. Select option **EV.U** (Event, User events) to open the User Selection panel shown in Figure 62.

   This panel is the starting point for finding the audit trail of one or more specific users, or finding events caused by some types of users.

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                zSecure Admin+Audit for RACF - Events - User Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Userid  . . . . . ________     (userid or EGN mask)
Owned by  . . . . ________     (group or userid, or EGN mask)
System  . . . . . ____         (system name or EGN mask)
Name  . . . . . . ____________________________ (name/part of name, no filter)
Installation data . ____________________________ (scan of data, no filter)
Jobname . . . . . ________     (job name or EGN mask)
Terminal  . . . . ________     (Terminal id or EGN mask)

Advanced selection criteria
/  User actions            _  User attributes         _  Date and time
_  Data set selection      _  HFS selection           _  Resource selection
_  DB2 selection           _  CICS selection          _  Omegamon selection

Output/run options
_  Include detail          _  Summarize              _  Specify scope
_  Output in print format     Customize title           Send as e-mail
     Run in background        Sort differently
```

Figure 62. EV.U User Selection panel

3. In the **Advanced selection criteria** section, select **User actions**, and press Enter. You now see a selection panel with the types of actions recognized.
4. Type a **/** in **RACF/CKGRACF commands** issued and another **/** in front of **Successful**. Then press Enter to open the RACF command overview panel shown in Figure 63.

   This panel shows you the successful RACF commands issued in your system. You can scroll right using PF1.

```
Event log record detail information                  1 s elapsed, 0.7 s CPU
Command ===> ____________________________________________ Scroll===> CSR_
                                              4Apr05 09:17 to  4Apr05 09:21
   Date      Time     Description
__ 04Apr2005 09:17:16 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:32 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:46 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:17:53 RACF SETROPTS success for IBMUSER
__ 04Apr2005 09:21:22 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:30 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:49 RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPT
__ 04Apr2005 09:21:55 RACF SETROPTS success for IBMUSER
****************************** BOTTOM OF DATA ********************************
```

Figure 63. RACF command event log records overview

5. To see more detail than just a one-line summary per record, select option **Include detail** in the **Output/run options** section of the User Selection panel (Figure 62) and rerun the query.

   In the RACF Event log overview panel, select a record to open the RACF command detail panel shown in Figure 64 on page 77. Now you can see the details; for example, the full command and fields identifying the user.

```
Event log record detail information                          Line 1 of 43
Command ===> ____________________________________________ Scroll===> CSR_
                                          4Apr05 09:17 to  4Apr05 09:21


  Description
  RACF PERMIT success for IBMUSER: PERMIT FACILITY $C2R.OPTION.HD.8

  Record identification
_ Jobname + id:  IBMUSER
  SMF date/time: Wed  4 Apr 2005 09:17:46.59
_ SMF system:    DEMO       record type:  80   record no: CKR1SM01 3013

  Event identification
  RACF event description        Permit command (Success:No violations detected)
  RACF event qualifier          0
  RACF descriptor for event     Success
  RACF reason for logging       Class Special
  SAF authority used            Special
  Audit/message logstring

  RACF command
  PERMIT '$C2R.OPTION.HD.8' ACCESS(READ) CLASS(FACILITY) ID(IBMUSER)
```

Figure 64. RACF command event log record detail panel

Tracking configuration changes

Note
This function is available only in zSecure Audit for RACF.

The Change Tracking function is a powerful way of ensuring that changes in sensitive RACF and SYSTEM definitions are tracked. You can list differences between the verified base and the current configuration.

There are different kinds of sensitive RACF definitions. Some examples are: system-wide SPECIAL users, OPERATIONS users, and profiles that protect sensitive data sets. SYSTEM-related sensitive definitions are, for instance, APF defined data sets such as `APFLIST`. You can also identify other RACF or SYSTEM definitions as sensitive in addition to those already marked as sensitive.

Other system settings that can be monitored include changes to the list of APF-authorized libraries and changes to the RACF Class Descriptor table. You can track changes to most items that zSecure Audit for RACF shows information about.

Tracked changes must be accepted or rejected, or deferred. You accept a change to update the verified base, or you reject a change because of an incorrect modification. If you reject a change, be sure to also undo the modification in your configuration; otherwise, during the next Change Tracking step, the same modification will be reported again.

Detecting library changes

Note
This function is available only in zSecure Audit for RACF.

Using the Library Change Detection function in a realistic manner requires a certain amount of planning and time. After reviewing the short description that follows, you can decide whether you want to use this function during your evaluation. The function is described, in detail, in the *Library Audit* section of the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

The Library Change Detection function provides a library update report that is used to find and display changes to members consisting of load modules or source text of partitioned data sets. It contains logic to track libraries on shared DASD, in a sysplex environment, and in an SMS-managed environment. The basic function is built around zSecure Collect data for every member in every library being monitored. All system libraries are usually included, though you can also exclude them, and you can specify other libraries to be monitored. zSecure Collect for z/OS examines each member of these libraries and computes a digital signature for the data in the member. This digital signature is recorded in the CKFREEZE data set produced by zSecure Collect for z/OS

Library change detection is very useful for internal auditors. Using the Change Detection function can be a powerful tool, especially for internal auditors. By comparing data from month to month or year to year, the auditor can identify every program, either source code or load module, changed during that period. This is not limited to system libraries: Application libraries can be monitored just as well.

The default CKFREEZE data sets, such as you created when building your current input sets, do not contain the necessary data for library management. You must submit another zSecure Collect for z/OS job to gather library member data. If you want to try this, use the **Freeze** option (Option **0**) in the Audit-Libraries panel shown in Figure 65 on page 79.

This option asks you for parameters and allows you to submit the necessary job. (The best option for you to select is probably **System Libraries**, but you can specify any libraries you want.) You can elect to reuse your existing CKFREEZE data set. The new CKFREEZE data set will have all the default data (from your z/OS tables but not from VTOC, VVDS, catalogs, etc.), plus the new library member data. This zSecure Collect for z/OS job takes a few minutes to run because it must open and read every member of the selected libraries.

```
  Menu   Options   Info   Commands   Setup   StartPanel
------------------------------------------------------------------------------
              zSecure Audit for RACF - Audit - Libraries
Option  ===> _____________________________________________________

0    Freeze          Calculate new digital signatures
1    Lib all         Overview of all libraries
2    Lib changes     Overview of all libraries with changes
3    Status          Show member status
4    Changes         Identify members with changes
5    Scan            Show members flagged by SCAN function
6    Duplicates      Identify identical members
7    Application     Members summarized by application
8    Prefix          Members summarized by member prefix (component code)
9    PTF - ZAP       Members touched by PTF or ZAP
```

Figure 65. Primary library update analysis panel

To perform library change detection, you must have multiple generations of CKFREEZE data sets, and define at least two in your input set. With some planning, GDGs are ideal for this purpose. zSecure Audit for RACF compares the signatures in the various CKFREEZE data sets and produces reports. Not all functions of library update analysis require two CKFREEZE data sets. Options 1, 3, 5, 6, 7, 8, and 9 can be used with just one or more CKFREEZE data sets. Other options are available as part of library monitoring. For example, zSecure Collect for z/OS can examine library members for specific text or hexadecimal strings anywhere in the member, or for usage of specific SuperVisor Calls (SVCs). This is a good way to answer the frequently asked question of which program is using an SVC.

These options are described in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*. During data collection for CKFREEZE, the hexadecimal searches can also be used to locate typical authorization code fragments. The option to identify duplicate members can be useful. It can detect library members in all the libraries scanned when the CKFREEZE data set was built with duplicate member names, or with duplicate contents regardless of the member name. There is no reasonable way to do either of these functions with standard z/OS utilities, yet detection of duplicate members is critical for effective software maintenance and for audit control.

To use the Library Change Detection functions, your input file setup might look similar to this example:

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
              zSecure Audit for RACF - Setup - Input F      Row 1 from 5
Command ===> _____________________________________________ Scroll ===> CSR_

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

   Description                                            Complex
_  CKFREEZE dd 4 Apr 2005                                          selected
_  CKFREEZE dd 8 Apr 2005                                          selected
_  Active primary RACF data base                          DEMO
_  Active backup RACF data base                           DEMO
_  Active backup RACF data base and live SMF data sets    DEMO
****************************** Bottom of data ********************************
```

Figure 66. Input set definition

This is a rather primitive input structure, but it can be used for evaluation. The SMF data set is not required for the library functions discussed here. You would

collect the OLD data first using the **Freeze** option to generate and submit the necessary job, and then collect the NEW data a few days later. For long-term use, you would probably use generation data groups, such as `'HLQ.CKFREEZE(0)'` and `'HLQ.CKFREEZE(-1)'`.

An input set can contain any reasonable number of SMF and CKFREEZE data sets, and one RACF database. The RACF database can be the active RACF database, unloaded RACF data, a copy of a RACF database, or an active RACF database from another system. It can consist of any number of data sets.

Chapter 10. Using resource-based reports on TCP/IP configuration, z/OS UNIX, CICS, IMS, and DB2

The Resource reports option (**RE**) available from the Main menu provides access to display and reporting options for the following RACF resources:

- TCP/IP configuration and statistics
- UNIX file system information and audit reports
- CICS® region, transaction, and program data
- IMS™ region, transaction, and program data
- DB2 region data

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                          zSecure Suite - Main menu
Option  ===> ____________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
  I    IP Stack        TCP/IP stack reports
  U    Unix            Unix filesystem reports
  C    CICS            CICS region and resource reports
  M    IMS             IMS control region and resource reports
  D    DB2             DB2 region report
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex: DAILY

Product/release:
5655-T01 IBM Security zSecure Admin 1.13.0
5655-T02 IBM Security zSecure Audit for RACF 1.13.0
```

Figure 67. zSecure Audit for RACF Main menu

For more information, see the following topics:

- "IP Stack reports"
- "UNIX filesystem reports (RE.U)" on page 83
- "CICS region and resource reports" on page 86
- "IMS region and resource reports" on page 89
- "DB2 region reports" on page 92

IP Stack reports

Use the **RE.I** option to select and display TCP/IP configuration and statistics data. This data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized with the `TCPIP=YES` parameter. You can also report on SMF events related to IP configuration data using the **EV.I** menu option.

When you select **RE.I** from the Main menu, the panel shown in Figure 68 is displayed.

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Resource - IP stack Selection
Command ===> ____________________________________________________   _ start panel

Show TCP/IP stack configuration data that fit all of the following criteria:
Stack name . . . . . _________ (name or filter)
System . . . . . _________ (system or filter)
Sysplex  . . . . . _________ (sysplex or filter)


Output/run options
_  Ports                  _  Rules                  _  VIPA
_  Interfaces             _  Routes                 _  Netaccess
_  AUTOLOG                _  Resolver
_  Output in print format  _  Customize title       _  Send as e-mail
  _  Run in background
```

Figure 68. IP stack Selection panel

From the IP stack Selection panel, you can limit the TCP/IP stack configuration data by entering selection criteria into one or more fields. When you specify selection criteria, only records that match all criteria are included in the output. Filters can be used in some of the selection fields. For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (PF1).

You can also specify Output and run options on the Selection panel. You can use the run options (Ports, Rules, VIPA, Interfaces, Routes, Netaccess, AUTOLOG, and Resolver) to specify additional selection criteria for specific types of IP configuration data. Use the output run options to specify report and print options. When you select any of these options, the corresponding panels are displayed when you press Enter on the IP stack Selection panel.

If you do not select any Output or run options, the data is processed as soon as you press Enter on the IP Stack Selection panel. An overview panel is immediately displayed with a summary of the IP configuration records that match the selection criteria you specified.

See the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* for more detailed information about these reports.

UNIX filesystem reports (RE.U)

When you select option **RE.U**, the Resource - Unix panel shown in Figure 69 opens.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix
Option  ===> ____________________________________________________________

F    Filesystem      Unix filesystem selection
R    Reports         Unix audit reports
```

Figure 69. Resource Unix Menu

Filesystem - Unix filesystem reports

Use this option to select and display UNIX file system records. A full CKFREEZE data set read is required, and the CKFREEZE data set must have been made with the `UNIX=Y` parameter. If the zSecure Collect run was APF-authorized, additional information is displayed.

When you select option **F**, the Resource - Unix Selection panel shown in Figure 70 opens.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> ____________________________________________   _ start panel

Show Unix files that fit all of the following criteria:
File  . . ____________________________________________________________
Complex . ________     (complex or EGN mask)

Advanced selection criteria
_  File attributes         _  File system             _  File ACL

Output/run options
_  Output in print format  _  Customize title         _  Send as e-mail
  _  Run in background
```

Figure 70. Resource Unix selection panel

If the selection panel is left blank, all UNIX files are selected. You can limit the UNIX files selected by completing one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields. You can select one of the Advanced selection criteria to specify filters to select and display UNIX files. When you select a criterion, a panel opens where you can specify the attributes in which you are interested.

Use the Output/Run options to customize settings to run the report and generate output. The settings you specify are saved in your ISPF profile and become the default settings for all UNIX panels that provide the option.

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

After processing the CKFREEZE file using the specified selection criteria, the UNIX summary panel opens to display the results as shown in

Figure 71.

```
IBM Security zSecure UNIX summary                            Line 1 of 26
Command ===> _________________________________________ Scroll===> CSR_
All Unix files                                     28 Aug 2008 00:07
   Complex System  Count
   EEND     EEND     70562
   Count FS mount point
__    24  /
__     2  /home
__     2  /home/crmbhg1
__   205  /u
__     5  /u/automount
__  1713  /u/automount/c2eaudit
__  3105  /u/automount/c2rnew
__   446  /u/automount/smpe
__   730  /u/automount/smpe/smpnts/STP82890/SMPPTFIN
__  1434  /u/automount/C2RSRV#P
__   283  /u/automount/C2RSRV#P/PZ00350
__     1  /u/automount2
__     1  /u/zosmapper
__    11  /EEND
```

Figure 71. UNIX summary display

Selecting any of the mount points listed in the UNIX summary panel (Figure 71) displays the list of UNIX files for that mount point as shown in Figure 72.

```
IBM Security zSecure UNIX summary                         Line 1 of 446
Command ===> _________________________________________ Scroll===> CSR_
All Unix files                                     28 Aug 2008 00:07
   Complex System  Count
   EEND     EEND     70562
   Count FS mount point
     446  /u/automount/smpe
   T FileMode +  apsl AuF Owner    Group    Relative pathname (within FS)
__ d rwx------        fff CRMBHJ1  ZSECUR   .
__ d rwx------        fff CRMBHJ1  LDAP     smpnts
__ l                  fff CRMBHJ1  LDAP     smpnts/zos19jpn
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XML
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XSL
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD/S0004.ESMCP
__ d rwx------        fff CRMBHJ1  ZSECUR   smpnts/STP82890/SMPPTFIN
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
```

Figure 72. UNIX summary panel - UNIX file list for selected mount point

You can perform the following actions from this panel:

- To browse the regular files, type **B** in the selection field for a file or directory entry.
- To call the UNIX System Services ISPF Shell for a file or directory, type **I** in the selection field for that file or directory.
- To start the z/OS UNIX Directory List Utility for a directory, type **U** in the selection field for the directory.

When you browse a file from the UNIX file list display panel (Figure 72), the UNIX file detail display panel shown in Figure 73 on page 85 opens. To

browse the contents of a file in this panel, type **B** in front of the **Absolute pathname** field.

```
IBM Security zSecure UNIX summary                          Line 1 of 57
Command ===> _____________________________________________ Scroll===> CSR_
All Unix files                                  28 Aug 2008 00:07



  System view of file
  Complex name                  EEND
  Sysplex name                  NLDLPPLX
  System name                   EEND
_ Absolute pathname             /u/automount/smpe/smpnts/STP82890/GIMPAF.XML
  FS mounted with SECURITY      Yes
  FS mounted with SETUID        No
  FS mounted READ/WRITE         Yes
  File access attributes        go=,u=rw
  Security label
  Extended file attributes      +s -apl
  Effective audit flags         =f
_ Owner name                    CRMBHJ1 CRMQA097 HZSUSER LDAPSRV OMVS RCCSL01
_ Owner name                    SKRBKDC STRCONS STRTASK TCPSRV
_ Group name                    LDAP SMPE
  Home Directory for Users
  Device                        1648
  Relative audit priority
  Audit concern

  Physical file attributes
  Complex that owns file system EEND
  System that owns file system  EEND
  File system data set name     CRMBOMVS.U.SMPE.HFS
  Volume serial for file system SMPNTS
  File system DASD serial + id  IBM-68-000000065892-0062
  Relative pathname within FS   smpnts/STP82890/GIMPAF.XML
  File type                     -
  Physical access attributes    o=,u=rw,g=r
  Physical extended attributes  +s -apl
  User-requested audit flags    =f
  Auditor-specified audit flags =
  User id                       0
  Group id                      3
  Inode number                  98
  File audit id                 01E2D4D7D5E3E2000F05000000620000
  Number of hard links          1
  Link target

  User     TOrwx ACL id   UID/GID    Name                 InstData
  CRMBHJ1   urw- CRMBHJ1  0          JOHN FRANK
  CRMQA097  urw- CRMQA097 0          TEST QUOTED FORMAT   OMVS HOME TO TEST $QU
  HZSUSER   urw- HZSUSER  0                               Z/OS HEALTH CHECKER
  LDAPSRV   urw- LDAPSRV  0          LDAP SERVER USER
  OMVS      urw- OMVS     0
  RCCSL01   urw- RCCSL01  0          JOHN SMEDLINE SPEC.
  SKRBKDC   urw- SKRBKDC  0          KERBEROS STARTEDTASK NETW AUTH KERBEROS
  STRCONS   urw- STRCONS  0          STC VOOR TSO CONSOLE
  STRTASK   urw- STRTASK  0          DIV STARTED TASK USR
  TCPSRV    urw- TCPSRV   0          TCPIP STARTED TASK
  -group-   gr-- LDAP     3
  -group-   gr-- SMPE     3
  - any -   o--- -other-  n/a



****************************** Bottom of Data ********************************
```

Figure 73. UNIX detail display

For more detailed information about these reports, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

Reports - running the predefined UNIX audit reports

Use the Reports option to generate any of the predefined UNIX audit reports available in zSecure. When you select this option, a panel opens with a list of reports for selection. See Figure 74. For details about a specific report, position the cursor on the report selection field, and then press F1 to view the online help.

```
zSecure Suite Display Selection                          3 s elapsed, 0.8 s CPU
Command ===>_____________________________________________ Scroll===> PAGE

  Name     Summary Records Title
_ MOUNT          0       0 Effective UNIX mount points
_ UNIXAPF        0       0 UNIX files with APF authorization
_ UNIXCTL        0       0 UNIX files that are program controlled (daemons etc)
_ UNIXSUID       0       0 UNIX files with SETUID authorization
_ UNIXSGID       0       0 UNIX files with SETGID authorization
_ GLBWUNIX       0       0 UNIX files vulnerable to trojan horse & back door at
_ UIDNOUSR       0       0 UIDs not defined in the complex
_ GIDNOGRP       0       0 GIDs not defined in the complex
_ SHRDUIDS       1     196 OMVS UIDs shared between RACF users
_ OMVSNUID       1      21 RACF users with OMVS segment but no UID
_ SHRDGIDS       1      42 OMVS GIDs shared between RACF groups
_ OMVSNGID       1       2 RACF groups with OMVS segment but no GID
****************************** Bottom of Data ********************************
```

Figure 74. Unix Reports listing

CICS region and resource reports

Use the **RE.C** option on the Main menu to select and display CICS region, transaction, and program data. The report data is obtained from a CKFREEZE data set that is created by running zSecure Collect APF-authorized.

When you select **RE.C**, the CICS Resource panel shown in Figure 75 is displayed.

The **T** and **P** options are features provided by the zSecure Audit products.

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                  zSecure Suite - Resource - CICS
Option  ===> ____________________________________________________________

R   Regions       CICS region reports
T   Transactions  CICS CICS transactions selection and reports
P   Programs      CICS programs selection and reports
```

Figure 75. CICS Resource panel

CICS region reports

In the CICS Resource panel in Figure 75, select the **R** menu option to display the CICS Regions selection panel in Figure 76 on page 87.

Use this panel to enter selection criteria in one or more fields to limit the CICS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (PF1).

You can also select output and run options in the CICS Regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS region records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                     zSecure Suite - CICS - Regions
Command  ===> ____________________________________________________________

Show CICS regions that fit all of the following criteria:
Jobname . . . . . . . . _________  (jobname or filter)
VTAM applid . . . . . . _________  (applid or filter)
SYSIDNT . . . . . . . . _________  (identifier or filter)
Complex . . . . . . . . _________  (complex or filter)
System  . . . . . . . . ____       (system or filter)

Advanced selection criteria
_  Region security settings  _  Region attributes   _  Classes

Output/run options
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

Figure 76. CICS Regions selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

CICS transaction reports

In the CICS Resource panel in Figure 75 on page 86, select the **T** menu option to display the CICS Transactions selection panel in Figure 77 on page 88.

Use this panel to enter selection criteria in one or more fields to limit the CICS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (PF1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options in the CICS Transactions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS transaction records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
               zSecure Suite - CICS - Transactions
Command  ===> ____________________________________________________________

Show CICS transactions that fit all of the following criteria:
Transaction . . . . . ____      (transaction or filter)
Program . . . . . ________  (program name or filter)
Jobname . . . . . ________  (jobname or filter)
VTAM applid . . . . . ________  (applid or filter)
SYSIDNT . . . . . ____      (identifier or filter)
Complex . . . . . ________  (complex or filter)
System  . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource
 Advanced transaction selection criteria
_  Security settings    _  Attributes


Output/run options
1  0. No summary        1. Summarize by region  2. Summarize by transaction
_  Print format            Customize title         Send as e-mail
      Background run       Full page form
```

Figure 77. CICS Transactions selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

CICS program reports

In the CICS Resource panel in Figure 75 on page 86, select the **P** menu option to display the CICS Programs selection panel in Figure 78 on page 89.

Use this panel to enter selection criteria in one or more fields to limit CICS program data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options in the CICS Programs selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS program records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
             zSecure Suite - CICS - Programs
Command  ===> ____________________________________________________________

Show CICS programs that fit all of the following criteria:
Program . . . . . ________  (program name or filter)
Program type  . . . . . 4  1. Program  2. Mapset  3. Partitionset  4. All
Jobname . . . . . ________  (jobname or filter)
VTAM applid . . . . . ________  (applid or filter)
SYSIDNT . . . . . ____      (identifier or filter)
Complex . . . . . ________  (complex or filter)
System  . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource
Advanced transaction selection criteria
_  Security settings    _  Attributes
Output/run options
_  0. No summary        1. Summarize by region  2. Summarize by program
_  Print format            Customize title         Send as e-mail
         Background run    Full page form
```

Figure 78. CICS Programs selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

IMS region and resource reports

Use the **RE.M** option on the Main menu to select and display IMS region, transaction, and program data. The report data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized.

When you select **RE.M**, the IMS Resource panel shown in Figure 79 is displayed.

The **T** and **P** options are features provided by the zSecure Audit products.

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                         zSecure Suite - Resource - IMS
Option  ===> ____________________________________________________________

R   Regions         IMS control region reports
T   Transactions    IMS transactions reports
P   PSBs            IMS program specification blocks
```

Figure 79. IMS Resource panel

IMS region reports

In the IMS Resource panel in Figure 79, select the **R** menu option to display the IMS Regions selection panel in Figure 80 on page 90.

Use this panel to enter selection criteria in one or more fields to limit the IMS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

You can also select output and run options in the IMS Regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the IMS region records that

match your selection criteria.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                          zSecure Suite - IMS - Regions
Command ===> ____________________________________________________________

Show IMS control regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . . ________   (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                Customize title        Send as e-mail
      Background run           Full page form
```

Figure 80. IMS Regions selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

IMS transaction reports

In the IMS Resource panel in Figure 79 on page 89, select the **T** menu option to display the IMS Transaction selection panel shown in Figure 81 on page 91.

Use this panel to enter selection criteria in one or more fields to limit IMS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS transaction selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS transaction records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - Transactions
Command ===> ____________________________________________________________

Show IMS transactions that fit all of the following criteria:
Transaction . . . . . ________  (transaction or filter)
Transaction class . . . ____    (class number or filter)
Program specif. block  ________  (PSB or filter)
Jobname . . . . . ________  (jobname or filter)
VTAM applid . . . . ________  (applid or filter)
IMSID . . . . . ____      (identifier or filter)
Complex . . . . . ________  (complex or filter)
System  . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings
Output/run options
0  0. No summary   1. Summarize by region  2. Summarize by transaction
_  Print format          Customize title      Send as e-mail
      Background run    / Full page form
```

Figure 81. IMS Transactions selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

IMS PSB reports

In the IMS Resource panel in Figure 79 on page 89, select the **P** menu option to display the IMS PSBs selection panel in Figure 82 on page 92.

Use this panel to enter selection criteria in one or more fields to limit IMS program specification block data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS PSBs selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS PSB records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - PSBs
Command ===> ____________________________________________________________

Show IMS PSBs that fit all of the following criteria:
Program specif. block   ________  (PSB or filter)
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . ________  (applid or filter)
IMSID . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . ________  (complex or filter)
System  . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced PSB selection criteria
_  Security settings

Output/run options
0  0. No summary        1. Summarize by region  2. Summarize by transaction
_  Print format            Customize title         Send as e-mail
      Background run    /  Full page form
```

Figure 82. IMS PSB selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

DB2 region reports

Use the **RE.D** option on the Main menu to select and display DB2 region data.

When you select **RE.D**, the DB2 regions selection panel shown in Figure 83 on page 93 is displayed.

Use this panel to enter selection criteria in one or more fields to limit the DB2 region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (PF1).

You can also select output and run options in the DB2 regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the DB2 region records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - DB2
Command ===> ____________________________________________________________

Show DB2 regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
Local LU name . . . . . ________          (luname or filter)
Local site name . . . . ________________  (name or filter)
DB2ID . . . . . . . . . ____              (identifier or filter)
Group attachment name   ____              (name or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

Figure 83. DB2 Region selection panel

For detailed information, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual* and the online help.

Chapter 11. Using CARLa commands

zSecure Admin and Audit for RACF ISPF panels generate commands that are sent to the products for execution. These commands are in the CARLa Auditing and Reporting Language (CARLa), a useful tool for systems programmers. This process is transparent to interactive users, but becomes important if you want to use product functions in batch mode. In general, the same CARLa commands can be used in either interactive mode or in batch mode. For example, you can use one of the primary options, the CO.C option, to specify CARLa commands directly.

Tip: Instead of typing **=CO.C**, you can also type the primary command **CARLA** at the command prompt on a panel to specify CARLa commands.

Many CARLa samples are provided with the products. When you have time, browse them at random and run the code samples that are interesting to you. You can also look at the index member CKA$INDX, which contains a list of all members in the CARLa library with a brief explanation. You can also browse the SCKRCARL library, which contains interactive ISPF and batch reports that you can use or tailor for your own needs. For more detailed information about CARLa and the SCKRCARL library, see the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.

Tip: To browse the SCKRCARL library, you can use the following steps:

1. Issue the `TSO ISRDDN` command from within the product under ISPF.
2. Type `F SCKRCARL` to look for the active SCKRCARL library.
3. Use the **B**(rowse) function to open the SCKRCARL library.

   The CKA$INDX member at the top lists the available members and their functions.

In addition to the manuals, IBM offers CARLa programming and customer enablement courses for frequent users of zSecure Admin and zSecure Audit for RACF. There is also a zSecure Customer Forum on developerWorks® at http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255. For links to this forum and other resources, see the **Community and Support** tab in the zSecure Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

You can use CARLa to define and format custom reports, using any fields known to RACF and SMF, with headings and line formats specified by you. Typical use involves identifying a pre-built display or report that is almost what you need, capturing and saving the CARLa used to generate the Display/Report from the Results panel, and modifying it to produce exactly what you need. zSecure Admin and Audit for RACF provides a whole library of sample CARLa material, the `CKRCARLA` library. You can add new members to this library, or create your own library. Do not alter the existing members of the library, because the interactive functions of the products use these members.

To run one of the members of the `CKRCARLA` library, complete the following steps:

1. Select option **CO** (Command) from the Main menu. Then press Enter to open the Commands panel shown in Figure 84 on page 96.

This panel is used to perform library commands.

```
 Menu         Options       Info    Commands     Setup           Startpanel
------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Commands
Option ===> ____________________________________________________________________

 1      Libraries       Select and maintain command library
 2      Members         Work with members from current command library
 3      Edit            Edit member from current command library
 4      Run             Run member from current command library
 5      Submit          Run member from current command library in background
 C      Command         Type in any CARLa command



 Member name . . . . ________     (If 3, 4 or 5 selected)
 Two pass query  . . N  (Y/N, option 4 only)

 Current library . . DD:CKRCARLA
 Input complex . . . Input set created 8 Apr 2005
 Current mask type . EGN
```

Figure 84. Commands (CO) used to run library commands

2. Select option **2** (Members) and then press Enter to select a member, or find the name of the member you want to execute in one of the user reference manuals.

   For this example, use member CKRLMTX3.
3. If you are using the Members function, find the member name (CKRLMTX3 or the member name you chose from the reference manual) in the Member list, or type the member name in the **Member name** field in the Commands panel.
4. From the members list, issue the **E** line command in front of the member you want to use (for example, CKRLMTX3). From the Commands panel, type option **3** (Edit) and press Enter.

   A panel opens showing the selected CARLa member as shown in Figure 85 on page 97.

```
EDIT       CKR.SCKRCARL(CKRLMTX3) - 01.00                        Columns 00001 00080
Command ===>                                                        Scroll ===> CSR
****** ******************************** Top of Data ********************************
=NOTE= Enter GO or RUN to execute commands, SUB or SUBMIT to generate batch job
000001  /*****************************************************BeginModule********
000002  * LICENSED MATERIALS - PROPERTY OF IBM
000003  * 5655-T01
000004  * Copyright IBM Corp. 1989, 2007
000005  * All Rights Reserved
000006  * US Government Users Restricted Rights - Use, duplication or
000007  * disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
000008  * File-stamp: <050621 MR 12:44:08 CKRLMTX3.SCKRCARL>
000009  * FMID: HCKR1C0 RMID: HCKR1C0 IBM Security zSecure Base 1.12.0
000010  * Purpose:
000011  *     List ACL matrix
000012  * Notes:
000013  *     Imbed this member after a selection newlist RACFSEL, e.g.:
000014  *
000015  *     n name=racfsel outlim=0
000016  *     select c=dataset s=base qual=SYS1
000017  *     sortlist qual
000018  *     i m=ckrlmtx3
000019  *
000020  * History:
000021  * 011015 1.2.0 SDG ERZ120: Created
000022  * 050621 1.7.0 MR  EZ0506016: Added execute & RACFSEL
000023  *****************************************************EndModule********/
000024
000025  n type=racf title='Data set access matrix'
000026   def alter(aclid,8,'Alter')
000027    subselect acl(access=alter and missing(whenprof))
000028   def control(aclid,8,'Control')
000029    subselect acl(access=control and missing(whenprof))
000030   def update(aclid,8,'Update')
000031    subselect acl(access=update and missing(whenprof))
000032   def read(aclid,8,'Read')
000033    subselect acl(access=read and missing(whenprof))
000034   def exec(aclid,8,'Execute')
000035    subselect acl(access=execute and missing(whenprof))
000036   def condacc(aclaccess,1,'C')
000037    subselect acl(exists(whenprof))
000038   def hdr_o('o',1,hdr$blank) true where((key='^')) /* always FALSE */
000039   def cond(aclid,'nditional')
000040    subselect acl(exists(whenprof))
000041
000042   select c=dataset s=base likelist=racfsel
000043   sortlist key(35) uacc alter control update read exec condacc,
000044   | hdr_o | cond
****** ******************************* Bottom of Data ********************************
```

Figure 85. Member CKRLMTX3 of the CKCARLA library

Update the data sets that contain the software only during installation and when applying maintenance. If you need customized members, store them in a data set of your own and use the configuration parameters WPREFIX or UPREFIX to use these data sets.

The CARLa program selected shows a matrix of the access granted on one or more profiles. It needs some customization for you to select the profiles you want to be reported on. To avoid changing the original member, this procedure shows you how to work with a temporary copy.

To customize the CARLa program, complete the following steps:

1. Issue the **CANCEL** command to be sure that you leave the edit session without making any accidental changes to the member.
2. Enter option **4** (Run). Because the needed customization has not yet been done, using this option results in a syntax error about an incorrect LIKELIST.

3. Press PF3 to open the Results panel. Then, enter an **E** before the **Command** line and press Enter. You are now editing a temporary copy of the CARLa program.
4. Customize the program:

   The customization required is documented in the **Notes**® section of the header. This program was created to be included from other programs. To include the program, write a selection newlist (lines 15 to 17), and include the program directly behind it (line 18).

   You can achieve the same result by adding the selection newlist to the start of the CARLa program:
5. Copy lines 15 to 17 directly after line 23. (Remove the * to uncomment them.)
6. Change the class (`c=dataset`) and HLQ (`qual=sys1`) specifications to match the profiles that you want to see.
7. Type **Go** or **Run** in the **Command** line to execute this program. A report similar to the one shown in Figure 86 opens.

```
BROWSE - IBMUSER.C2R10FE.REPORT ------——------------- LINE 0000 0.5 s CPU, RC=0
 COMMAND ===>                                            SCROLL ===> CSR
******************************** Top of Data ********************************
P R O F I L E   L I S T I N G    4 Apr 2005 00:50
Access matrix

Profile key                       UACC    Alter    Control  Update   Read
SYS1.*.**                         READ    SYS1                       C#MA
                                          SYSPROG
                                          P390
SYS1.*.MAN*.**                    NONE    SYSPROG  STRTASK           C#MBRACF
                                                                     C#MARACF
                                                                     C#MBDSCT


SYS1.BRODCAST                     NONE    SYSPROG           *
                                                            C#MBWTK
                                                            C#MBWT3
SYS1.CMDLIB                       READ    SYS1                       C#MA
                                          SYSPROG
SYS1.C#M.LINKLIB                  READ    SYS1                       C#MA
                                          SYSPROG
SYS1.CSSLIB                       READ    SYS1                       C#MA
```

Figure 86. CARLA access matrix

Instead of running one of the existing samples, you can program your own CARLa program. In the following example, run a small CARLa program to see what CARLa programming can mean to you.

To create a sample CARLa program, complete the following steps:

1. Select option **CO** (Command) from the Main menu to open the Commands panel shown in Figure 84 on page 96 so that you can run library commands.
2. Select option **C** (Command) to open the PDF editor.
3. In the editor workspace, type the following CARLa statements, changing *c#mb* to some RACF group in your system that owns userids.

```
newlist type=racf file=ckrcmd nopage
  select class=user owner=c#mb segment=base
  list 'alu' key(8) 'owner(newowner)'
```

Figure 87. CARLa example program

This small CARLa program generates RACF commands to change the owner. All user profiles currently owned by *c#mb* are selected and the owner field will be changed into `newowner`. The output (RACF commands) is written in the CKRCMD file and can be processed by the RUN command. See "Using the Results panel" on page 58.

The output is similar to the output shown in Figure 88:

```
/* CKRCMD file CKR1CMD complex DEMO NJE JES2DEMO generated 27
alu C#MBHEN  owner(newowner)
alu C#MBERT  owner(newowner)
alu C#MBJVO  owner(newowner)
```

Figure 88. CARLa example program output

To save this CARLa program for later use, you can copy it into your own private data set.

To copy the program, type the command **C9999** over the line number field of the first CARLa line. Then, enter CREATE in the command area. You now use the normal ISPF Edit function to create (or replace) members in a PDS.

Whenever you want to rerun your saved CARLa program, complete the following steps:

1. Type **CO** from the Main menu and press Enter.
2. Type **1** (Libraries) from the Commands panel and press Enter.
3. Type **I** (insert) line command in any detail line and press Enter to insert a line.
4. Type the name of your private library, use quotation marks if necessary and press Enter.
5. Select the library with the **S** line command and press Enter.
6. Press PF3 to return to the Commands panel.

   The name of your library is displayed in the **Current® library** field.
7. Type the member name of the CARLa program in the **Member name** field.
8. Select option **4** (Run).

Chapter 12. Performing typical administration and audit tasks

The following section discusses how to perform typical administration and audit tasks in Security zSecure Admin and Audit for RACF.

Removing a user

If you want to remove the RACF access credentials for a user and do not know the userid, you can use the zSecure Audit for RACF RA.U option to enter a name search pattern to locate the userid and determine which data sets the user can access. Then, you can select the user profile for removal.

To remove a user, complete the following steps:

1. Enter **RA.U** in the **Command** line to open the RACF User panel.
2. In the **Programmer Name** field, type the user name or name pattern to display all user profiles that match the name somewhere in the **Programmer Name** field.
3. Press Enter to display the results.
4. To remove the user from RACF, type **D** in front of the user profile and then press Enter.

Displaying which data sets a user can access

To list all data sets that a particular user can access, use the RACF Report Permit/Scope function (option RA.3.4).

Auditing load libraries

The Audit Library functions, Option AU.L in zSecure Audit for RACF, can easily detect situations that are difficult to detect with standard z/OS or RACF tools.

These situations, in both load libraries and source libraries, include:

- Whether the load libraries are clean, especially the system and APF libraries.
- Whether a module is present multiple times, under different names and perhaps under different owner profiles.
- Whether the same module is present in more than one library.

  Note: It would cause serious problems if one copy is obsolete, but is unknowingly called by some jobs due to the library search order.

Printing display panels

While you are examining the output of a Display function, you might want to print the data. Use the PRT command. Output goes to the ISPF LIST data set. For more complex reports, use the RESULTS command to review all the files produced by the last function. You can also print from this panel.

Finding profiles based on search criteria

The Match function can be exceptionally useful. This function finds all profiles that cover a specified data set or sets, or general resources. You can find this function in the following panels:

- Dataset profiles, option **RA.D** Data set
- General Resource profiles, option **RA.R** Resource
- RACF Report match, option **RA.3.7**

For **RA.D** and **RA.R**:

- **3 Match** treats the profile field as a resource name and selects the best profile that could match the resource name. (See the **BESTMATCH** parameter in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.)
- **4 Any match** treats the profile field as a resource name and selects all profiles that could match the resource name. (See the **MATCH** parameter in the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*.)

RA.3.7 works like **Any match**: The profile used by RACF is shown in the first line. The other profiles are used if the first profile is removed. Poor planning or administration can result in several profiles with different access lists and UACC values covering a data set.

Verifying a Protect All environment

You might be thinking about going to a Protect All environment. Most z/OS installations do so, although there can be much work involved. Try the Verify function of Protect All. If you use `SMS` or `HSM` or `ABR`, you might exclude the volume `MIGRAT` on the submenu of the Protect All function. This action can greatly reduce the number of unwanted messages. Especially in a RACF environment without `PROTECT ALL`, this Verify function can be very helpful. It outlines the work to be done in going to Protect All, and provides an inventory of all data sets that do not have RACF protection.

Using the Command function

Try the Command function (Option CO on the primary panel). See Chapter 11, “Using CARLa commands,” on page 95 for information.

Appendix A. Frequently asked questions

This section provides a list of frequently asked questions along with detailed answers.

Table 12. Frequently Asked Questions

Q: Why is the Main panel empty?

A: You need READ access to the CKR.** profile in the `XFACILIT` class. CKR** profiles can allow or prohibit the use of functions.

Q: I am still not sure which functions are for zSecure Admin and which are for zSecure Audit for RACF. How can I separate them?

A: You can check the *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*. With every function, the manual shows a check box indicating which product it supports. You can also add, for example, `LIMIT FOCUS=AUDITRACF` to the preamble `SETUP PREAMBLE`(SE.3) to limit the usable function to those in the zSecure Audit only.

Q: How can I generate the `DEFINE ALIAS` as part of the `COPY USER` action?

A: The catalog information is from the CKFREEZE data set. So you must include a CKFREEZE data set in the set of input files that you use. To create a CKFREEZE data set, use the option `SETUP NEWFILES` from the panels to generate the JCL. Save this JCL and run it early every morning using OPC/A or a similar product. The CKFREEZE data set can be very large, so use SYSIN parameters to reduce its size. First, try creating a large CKFREEZE, running it with APF, and specifying no parameters.

If running zSecure Admin with this CKFREEZE setting is too slow, add parameters: `VTOC=NO,CAT=MCAT,BCD=NO,MCD=NO,TMC=NO,RMM=NO,UNIX=NO`. You still need the bigger CKFREEZE if you want to delete users, including their data sets.

You can also enter the line command **MT** (manage TSO) in front of a User profile in the RA.U option. You can then define the alias and the ISPF profile data set for an existing user. With this alternative, however, you must know the name of the catalog to which you want to add the user's alias.

Q: Can I collect information of unloaded RACF and CKFREEZE files on different systems and send this information to one system for display and analysis?

A: Yes, if all systems are licensed. This is a typical way to use Security zSecure Admin and Audit for RACF.

Q: The output from my **L** line command does not match the information that is reported by zSecure Admin and zSecure Audit for RACF. What is wrong?

A: Check the input RACF data source. You are probably reporting from a RACF unload, whereas the **L** line command always shows the information from the active RACF database.

Q: How do I handle a shared JES2 spool environment, with one RACF database and several z/OS images?

Table 12. Frequently Asked Questions (continued)

A: Run the RACF unload once, from any system unless you want to work with live RACF data, and run multiple zSecure Collect jobs, one on each system. You can use the `SHARED=NO` parameter with the second or additional zSecure Collect for z/OS job to reduce the size of the resulting CKFREEZE data sets. You can do this only if your UCBs are properly defined with `SHARED` options to exactly reflect the sharing environment. Otherwise, zSecure Collect for z/OS processes everything. Create an `INPUT SET` that has these multiple CKFREEZE data sets defined.

Q: When should I use my live RACF database with zSecure Admin and zSecure Audit for RACF, when should I use unloaded data, and when should I use an old database copy?

A: Use the live RACF database for simple *ad hoc* inquiries and day-to-day routine RACF administration. Use an unloaded copy of the RACF database when (a) you intend to do extensive analysis work, and (b) you have no immediate intention of changing RACF data. When you are planning to use the Recreate function, be sure to run from an old database copy, because an unload database does not contain passwords. If you are working with RACF data from another system, this is unloaded data unless the RACF database for the other system resides on shared DASD and is accessed directly as a normal data set. As an oversimplified statement, an *administrator* typically works with the live RACF database, while an *auditor* typically works with an unloaded copy.

Q: I have produced a report that contains double lines for all reported profiles. What can cause this problem?

A: There are two possibilities that can cause this problem. If you have created this overview using the panels, then the double lines might be caused by selecting two RACF data sources in the SETUP application. When you are using CARLa, this same problem can be caused by forgetting to specify the keyword `SEGMENT=BASE` in the `SELECT` statement.

Q: I used the SETUP INPUT options to define my input sets. The next time I used zSecure Admin and zSecure Audit for RACF, my setup values were not saved. Why?

A: You might have used a different TSO userid the second time. The setup information is saved in your ISPF profile, and each TSO userid has its own ISPF profile data set. Also, there is a `SETUP` option to use the input files you last used. Look at the `SETUP RUN` to determine the setting of this option.

Q: Security zSecure Admin and Audit for RACF inspects many z/OS controls for various reports. When do the products obtain these controls from z/OS storage, and when should you use a CKFREEZE data set?

A: For *full* checking, Security zSecure Admin and Audit for RACF uses z/OS control blocks that are copied into the CKFREEZE data set. While this is more complex than simply using in-storage z/OS data, it produces much more consistent results. The results are meaningful for the time at which the CKFREEZE data was collected. For this reason, you might sometimes want to collect CKFREEZE data when your system is fully loaded and most active. This also means that you can perform studies on remote z/OS systems, using a CKFREEZE file and RACF unloaded data created on the remote system.

Q: I prefer to use an unloaded RACF database for my analysis work. When I find something that needs to be corrected, I normally use the RACF commands generated by zSecure Admin and zSecure Audit for RACF, which I sometimes edit, to correct the problem. However, my unloaded RACF database represents historical data. How do I know if the same problem still exists in the live RACF database?

Table 12. Frequently Asked Questions (continued)

A: Before submitting any significant change to RACF, switch to the live RACF database using a different *input* set in the Setup panels, and repeat the display that detected the problem. If the problem still exists, then execute the RACF changes.

Q: Some panels, such as the `AUDIT STATUS` panel, differentiate between full CKFREEZE data sets and some other type of CKFREEZE data sets. What is this?

A: Using the instructions in this evaluation guide, when you defined *new input* files and ran the Refresh job, you created a full CKFREEZE data set. In very large or widely distributed installations, a CKFREEZE data set can be large, and you might want to save multiple CKFREEZE data sets for audit and comparison purposes. There are options in zSecure Collect for z/OS to gather only part of the potential CKFREEZE data. Multiple CKFREEZE data sets are useful, for example, if you use the freeze functions to detect changes in various libraries, or if your auditors want system snapshots at certain defined times.

Q: I want to clone a user using the RACF/MASS UPDATE/COPY USER function, but the target, which is a new user, is already defined. How is this handled?

A: Assuming that you want to keep some of the permissions of the existing target user, use the Copy function, and type a **/** before **Generate RACF commands when the target user exists**. This action leaves existing permissions of the target, provided they do not conflict with authorities of the source user. If a conflict occurs, then the final authority rests with the source or target user, depending on the exact commands (add versus alter). The target user might have some of its existing authority levels reduced because the source user had these lower levels.

Q: I get message CKR0536 when I attempt to copy to an existing userid.

A: If your intent is to have the set of commands as a basis to start editing, then you can suppress the message by putting a **/** before **Generate RACF commands when the target user exists**. The standard way to merge user attributes is to use MERGE.

Q: I need to perform daily security administration. What RACF data source should I use?

A: For daily security administration, use an up-to-date RACF database. This database can be the active primary RACF database or the active backup RACF database. Changes to the active primary database are immediately replicated to the active backup RACF database. Because the active backup database is not used to perform access verification processing, it is a good practice to use it as the input data source. This practice does not degrade the performance of the RACF database when executing the access verification process for the other users of the system while you are running reports.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

Printed in USA

GI11-9162-00